FORT
Routing Technology
for a Free and Open Internet

Routing Security in Latin America and the Caribbean

NIC MÉXICO

lacnic

Table of Contents

Acknowledgments

Author:
Augusto Luciano Mathurin

Supervisors:
Carolina Caeiro
Guillermo Cicileo

Reviewers:
Carlos Martinez-Cagnazzo
Raúl Ramirez Castañeda

Style Editor:
María Eugenia Martínez

Graphic Designer:
Martin Mañana

English Translator:
Justina Díaz Cornejo

Collaborators:
Andrei Robachevsky
Gerardo Pias
Mariela Rocha

Introduction

Routing is one of the few components of Internet infrastructure that is still insecure. Nowadays, it is easy to hijack routing systems to block websites, spy on users and redirect traffic to false destinations. These vulnerabilities may affect the free flow of information around the world and pose a threat to the security and privacy of users.

Internet standardization bodies have been struggling for a long time to identify strategies that make routing more secure. The purpose of this three-part report is to help us address and understand this issue both globally and in our region.

- Firstly, as an introduction, this report explains that the Internet can be the target of various attacks of very diverse technical characteristics, and then moves on to routing infrastructure attacks that become incidents: hijacks and leaks in the BGP protocol.
- It then provides an exhaustive analysis of incident data collected in 2017, 2018 and part of 2019. This is to understand —on the basis of statistics that can be studied by country— how routing security has evolved in the last few years. Statistics help us get a grasp of how our region compares to the rest of the world and actually show how these incidents may affect Internet freedom.
- Lastly, it outlines the various measures that network operators can adopt to enhance the Internet routing system. Mainly, the implementation of a public key infrastructure for resource certification (RPKI), which has been the most successful initiative in securing BGP routing.

This report is part of a RPKI deployment campaign in Latin America and the Caribbean, promoted by the FORT project, a joint initiative of LACNIC and NIC.MX, which seeks to improve routing system security and resilience.

What is at Stake?

Tip!

This section aims at introducing technical concepts and topics that provide the report with context. If you are knowledgeable about network operation, you can skip this part and go straight to the "*Incidents Timeline*" section.

Cyber-attacks are not new. They began as a few incidents that made amazing news headlines, but they are now part of the daily news: the week's blocking, data breach, malware or attack.

Some governments seek to prevent their citizens from communicating freely through the Internet,[1] for cultural and historical reasons, to avoid organized demonstrations or incidents, to hide uncomfortable truths or simply to keep the upper hand on the population in the name of security and social wellbeing.

Criminal associations engage in online massive scams and even some organizations try to sabotage their competition. But, how can there be *attacks* on the Internet?

To answer this question, we first need to think what the objective of the attacker is or, in other words, which quality of the information they want to affect. It is possible to attack the confidentiality (which translates into espionage attacks), the availability (which results in censorship) or the integrity (which devolves into fraud) of information.

Once the objective has been set (*what* to attack), the strategy is planned (*how* to attack) and, as is often the case, it is possible to reach the same destination (to accomplish the objective) through different paths. Internet architecture is complex, and different attacks can be carried out at several different levels or layers and they evolve with time. At the same time, the security measures to mitigate them are being perfected.

As regards censorship, which is the most common goals, there are different types of technical strategies to carry it out.[2] The most famous are:

- Blocking the access to certain IP addresses. For instance, an ISP can prevent its clients from accessing a certain site, discarding all of the requests whose destination is the IP address that corresponds to the servers where the blocked portal is hosted. This technique can also be used from the other end; i.e., a server that rejects the requests coming from an IP set. For example, the ones that belong to a certain country.
- DNS filtering. Generally, ISPs offer their own DNS resolver server; i.e., the service that translates URLs or domains (like www.lacninc.net) into an IP address (in this case, 200.3.14.184). It is possible to block domains that belong to the sites an attacker wants to censor. This way, clients

---

[1] <https://www.maketecheasier.com/internet-censorship-block-citizens-from-websites/>

[2] <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-internet/>

are not able to reach their intended destination. This technique can be easily avoided by changing the device's DNS resolver server, although nowadays most of DNS queries are not made using encryption. This means that providers can also set filters even when queries are not sent to their DNS servers.

- URL filtering. When clients connect to the Internet through a proxy server, it is possible to filter the addresses or URLs of websites that contain certain words.
- The "kill switch" solution is also possible. This means turning routers off using software (through malware) or physically unplugging them. This way, it is possible to deprive a population of Internet access or to take down a server.
- Content removal. Sometimes, it is not necessary to censor an entire web portal, but just to somehow force it to stop showing certain content. This technique is the most commonly used when resolving some legal disputes, such as copyright infringement.
- Denial-of-service attacks. Another way to shut down a server is to saturate it by redirecting an irrational amount of garbage traffic to it.

This list is not exhaustive. It simply aims at providing a notion of the range of potential or existing attacks. This report focuses on the attacks that happen in another part of the Internet infrastructure: the routing layer.

Akin to a road network, the Internet has its own highways and crossroads, which are cables and routers. When driving, we use a GPS, a driver-assistance system to know how to get from point A to point B, driving on all the necessary routes and making the necessary stops. Similarly, the Internet uses its own navigation system, called BGP (Border Gateway Protocol), which makes it possible for data traffic in the network to reach its destination.

Just like most of Internet protocols, the BGP was created toward the end of 1980s, in a scenario that was very different from the current one. At the time, only a small number of networks needed to be connected. Back then, security was not a core principle to have in mind, so the protocol was strongly based on a trust game between the parties.

Things are different today. With over 92,000[3] registered autonomous systems that are part of this Internet navigation system, it can no longer be assumed that all of its participants are trustworthy. Certain actors may even be rivals, like two competing ISPs that offer their services to the same population. How is this scenario harmful to Internet users?

Back to the road network analogy, if cables are the roadways, then the BGP would be the road sign system; i.e., all the signs that indicate which roads to take in order to get to the desired destination. The problem with —and, at the same time, the advantage of— the Internet is that there is no central body to manage it, so it is impossible to control who places the signs on this road network or whether their indications are authentic. This is the so-called BGP trust game, and it can be used to carry out attacks, censor, and spy on users.

When we visit a website, both endpoints (our device and the server hosting the portal) have an IP address that allows their identification. Thus, data packets have a source and a destination, but what happens on the way?

---

[3] <https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html>

In the postal system, letters are not sent straight to their destination, but to intermediaries, the post offices.[4] When using this system, the letter goes to a local post office and may go through several intermediary post offices until it arrives at the city where it will reach its final address. On the Internet, when data packets are sent from our device to the desired endpoint, these are first sent to the "post offices", i.e., the autonomous systems.

An autonomous system is a network or a network set managed by an organization and has a common routing policy. Generally, autonomous systems are ISPs or organizations that connect multiple ISPs. Just like devices connected to the Internet are identified with an IP address, autonomous systems are identified with a 16- or 32-bit number, called ASN (Autonomous System Number).

Each autonomous system announces the IP prefixes (address sets) to which it is connected and can transmit information; the other autonomous systems can build their routes on the basis of these announcements to ensure the information packets they transport reach their destination. This makes the BGP a powerful and flexible protocol, which allows for the interconnection of networks to be updated dynamically, achieving a manageable route exchange and a quick response in case one of the routes becomes unavailable.

However, as mentioned above, the BGP was not designed from a security perspective, which makes it vulnerable to certain attacks. An autonomous system can announce routes to an IP address prefix that is not actually under its control, and if these announcements are not filtered, they can be spread across the network. In this case, all the traffic intended for these IP addresses would be directed to the autonomous system that made the false route announcement. This threatens the free development of the Internet; strategies complementary to the ones we have already mentioned can be devised to censor or conduct surveillance.

The most iconic routing incident on the Internet happened in 2008,[5] when the Pakistani government ordered to block YouTube, the video-sharing platform. When the country's public ISP received this order, it configured its autonomous system so that connections with YouTube's IP addresses as a destination were discarded. The objective was for local requests regarding this portal to be sent to a "black hole", blocking access and preventing the Pakistani people from visiting the platform. But these false prefix announcements were leaked outside Pakistan and scattered across the network. Suddenly, all YouTube requests were redirected to Pakistan Telecom, blocking the site in many parts of the world for hours. This wreaked havoc on the operation of the ISP due to the large amount of traffic it received.

It has been over 10 years since this incident happened. While the Internet is now more resilient —thanks to the lessons learned from this type of events—, routing infrastructure is still targeted to curtail the freedoms or alter the services of its users.

---

[4] ‹https://www.cloudflare.com/learning/security/glossary/what-is-bgp/›

[5] ‹https://dyn.com/blog/pakistan-hijacks-youtube-1/›

Types of incidents

In order to understand the different types of incidents that can happen on the Internet routing layer, it is necessary to fully understand how the BGP works. This protocol establishes the communication among autonomous systems that are configured to announce and/or learn routes, which allows destinations to be reached. In order for the route process to be more controlled, there are measures like filters or policies that can be adopted.

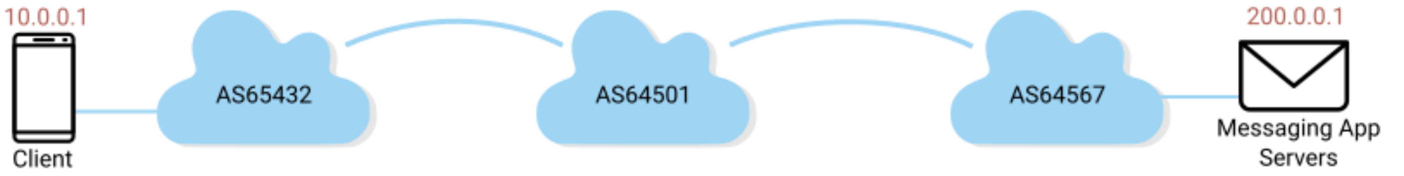
However, trust on the Internet lies in the fact that each organization should only announce its own prefixes or the prefixes of the organizations it brings transit to. However, this is not guaranteed under the BGP, since it is based on trusting the operators in different networks.

Whether involuntarily or intentionally, routing devices can have an unexpected behavior and announce a prefix that they are not supposed to announce. This is called a *routing incident* and can be classified into two major types: hijacks and leaks.

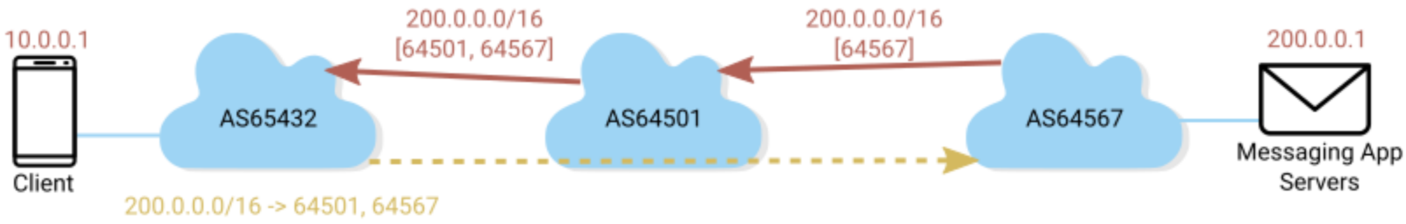
Let us imagine we want to connect to a messaging service via an app. Both our mobile device and the app server must be connected to the Internet and there must be a route allowing the flow of information between both endpoints.

We now know that both endpoints will not be directly connected to each other, but each will be connected to an autonomous system. These autonomous systems belong to the ISPs contracted by each endpoint to obtain connectivity. In this case, our mobile will be assigned the 10.0.0.1 IP address and our provider's ASN will be 65432, while the app servers will be connected via the 200.0.0.1 IP address and their autonomous system's ASN will be 64567.

Each autonomous system can be connected to other autonomous systems; these, in turn, can be connected to others, and so forth. Let us say that, in this example, there is only one network in-between.



How does AS65432 —the one connecting us— manage to know where to send the data packets so that they reach the 200.0.0.1 IP address? This is when the BGP comes into play. AS64567, owner of said IP address, announces that it has the corresponding prefix. This way, AS64501, which provides transit to the other two systems, announces route 64501 64567 to our AS65432 to reach network 200.0.0.0/16.

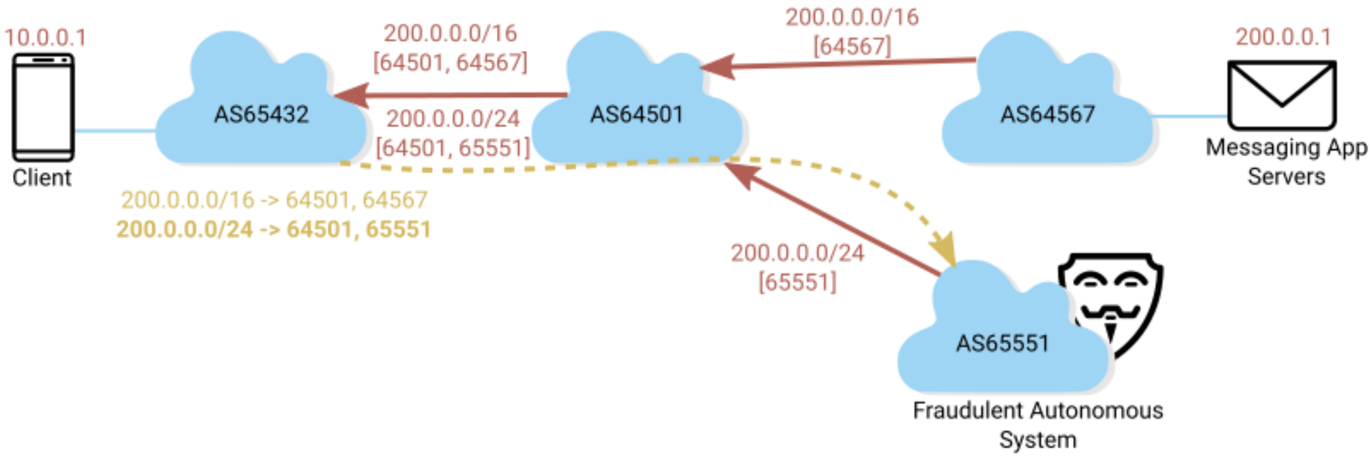


Thus, when our device wants to send information to the 200.0.0.1 address, AS65432 will already have the appropriate route to transmit the data from our mobile to the app servers. Similarly, AS64567 will be able to obtain a route to reach our IP address.

Route Hijacking (BGP Hijacking)

The case mentioned above is an example in which no incidents occur. But, what happens when we add a fraudulent AS that wants to hijack a route? "Route hijacking" is the act of announcing unauthorized prefixes to the Internet. This undue announcement may be intentional or an operational error, and it manages to be spread because it offers "a better route". The announcement provides a more specific prefix than the one announced by the original AS or it provides a shorter route, whether it exists or not.

Coming back to our example, let us say that there is a malicious operator that wants to block access to our app. To do this, it announces that it has a more specific prefix that contains the 200.0.0.1 address (in this case, 200.0.0.0/24).

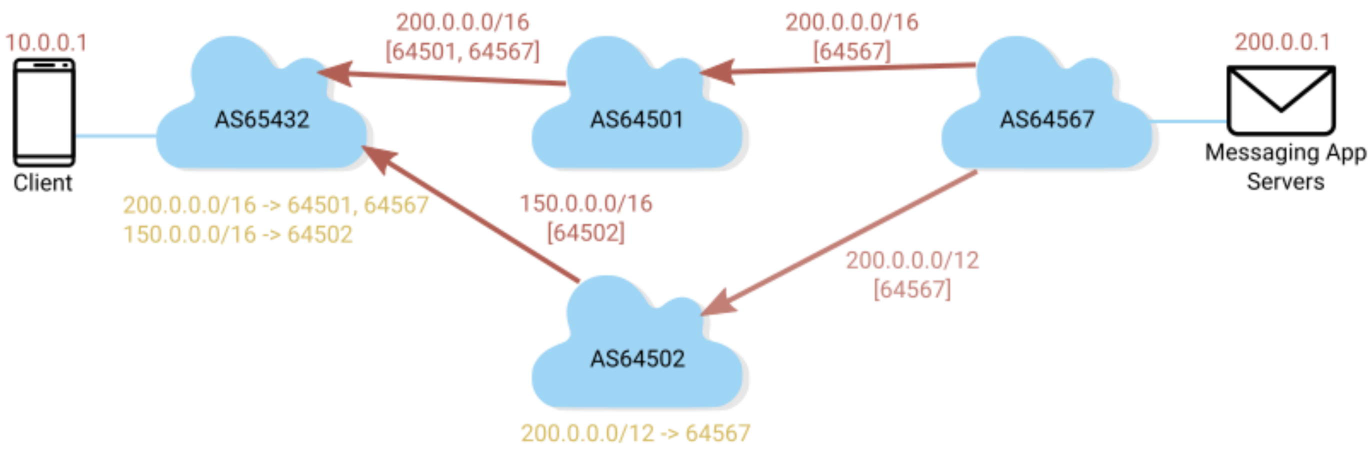


Therefore, the autonomous system that provides us with connectivity receives two different routes leading to the same destination and it ends up choosing the more specific one: i.e., the one from the fraudulent AS.

Route Leaks (BGP Leaks)

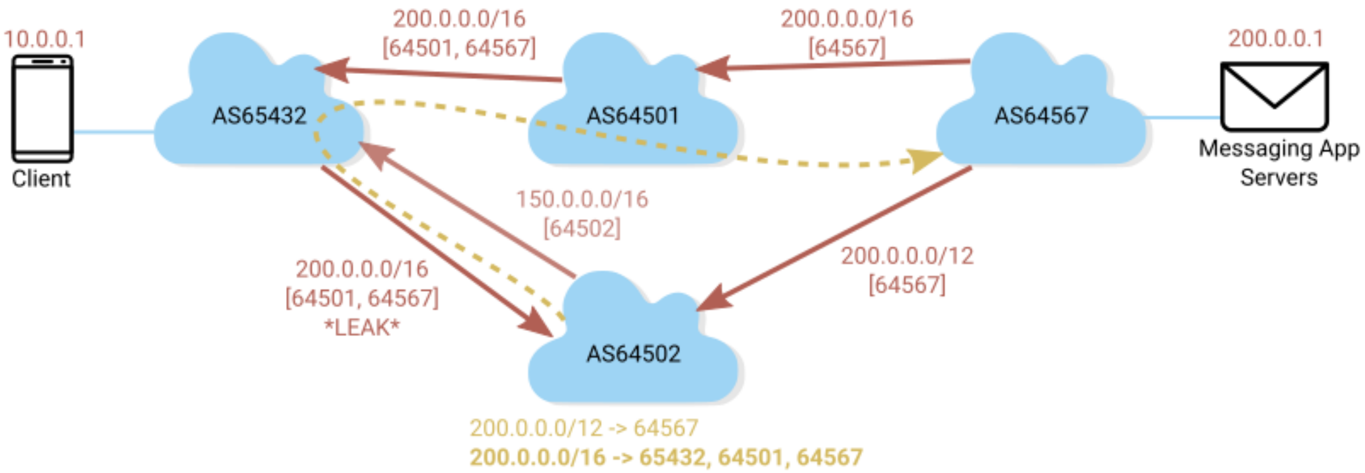
Leaks are another type of incident. When a routing announcement is spread and exceeds its desired scope, i.e., violates the policies of the issuing or receiving system or any other system that is part of the route, there is a route leak.[6] Generally, this happens when a network operator with multiple upstream providers above it accidentally announces to one of them that it has a route to the destination through another upstream provider, making the initial operator an intermediary between its two providers.

Coming back to our initial example, let us now suppose that AS65432, which provides us with connectivity, has two providers: AS64501, which we already know, and AS64502, which allows it to reach the 150.0.0.0/16 network. In turn, this autonomous system is connected to AS64567, although it is in theory irrelevant to our AS, since it reaches this destination via AS64501.



However, due to some configuration error, AS65432 announces the route with the 200.0.0.0/16 destination to AS64502. This is not an expected behavior, since our AS is a client, not a transit provider. The routing announcement exceeds its desired scope and creates a BGP leak. AS64502 does not filter this announcement and it now has a more specific route in order to reach 200.0.0.1 (200.0.0.0/16 through AS65432, against 200.0.0.0/12 through AS64567).

[6] RFC 7908



Despite the fact that the route is longer, the prefix is more specific, so AS64502 will start sending data flows to AS65432, which can cause network performance issues and even service cuts, both in the ISP providing us with connectivity and for the different clients wishing to access the messaging app.

Incidents Timeline

While incorrect BGP announcements happen every day causing small incidents, some wreak havoc globally for considerable amounts of time. Here is a list of some of the incidents that made the news due to their impact.

April 1997[7]
The AS 7007 incident was an important Internet disruption and the first routing incident to be reported globally due to its impact. April 25, 1997 started with a router operated by autonomous system 7007, accidentally announcing a substantial part of its routing table to the entire Internet and causing a "black hole" by redirecting content, causing it to go nowhere.

February 2008
The Pakistani government tried to censor YouTube via its public ISP by updating the BGP routes that led to the site. In addition, these announcements were sent to higher-tier providers and were spread across the Internet, causing all YouTube requests to be sent to Pakistan Telecom, which blocked access to the portal all around the world.

November 2012[8]
An error caused by an unexpected hardware failure in Moratel's equipment (ASN 23947), an operator in Indonesia, created a BGP leak and caused disruptions and issues to access Google services for 27 minutes.

November 2013[9]
Dyn Research showed evidence that the Internet traffic belonging to financial institutions, governments and ISPs was rerouted in various occasions to unauthorized places. It was suspected that this traffic might have been monitored or altered before reaching its destination.

August 2013[10]
For six days, the Italian web host Aruba S.p.A fraudulently announced its ownership of 256 IP addresses. This was done under the direction of the hacking and special operations team of the Italian military police to monitor the computers of different targets.

September 2014[11]
A Pennsylvania-based hosting company, VolumeDrive (AS46664), created a routing leak that caused disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.

March 2017[12]
Brazil's SECW Telecom fraudulently announced prefixes from Cloudflare, Google and Banco do Brasil and generated some service cuts across the region.

April 2017[13]
Part of the network traffic belonging to Master Card, Visa and many other financial services companies was rerouted through Rostelecom, a Russian provider. For several minutes, it fraudulently announced over 50 prefixes that belonged to other AS's.

August 2017[14]
Google accidentally leaked the prefixes its AS learned from peering relationships, becoming thus a transit provider. This caused large-scales Internet disruptions. Users in Japan were the most affected ones, with slow connections or disrupted connections for tens of companies in the country.

October 2017[15]
Due to a BGP leak, the traffic of multiple important CDNs was rerouted to Brazil. This caused setbacks for services like Google and Twitter for at least 20 minutes.

November 2017[16]
A Level 3 routing leak led to a service degradation in North America for over 90 minutes.

December 2017[17]
High-profile portals like Google, Apple, Facebook, Microsoft and Twitch, among others, were rerouted to a previously unused Russian AS. This was due to two BGP routing incidents that lasted only a few minutes.

April 2018[18]
A Russian provider announced IP prefixes fraudulently, which belonged in fact to Route53 Amazon DNS servers. This allowed a group of hackers to reroute a cryptocurrency portal to a fake site that stole credentials. This way, the group was able to steal approximately 152,000 US dollars' worth of cryptocurrencies.

July 2018[19]
In parallel with the different strategies from the Iranian government to censor networks like Telegram and Instagram, the AS belonging to the Iranian public telecommunications company fraudulently announced prefixes that belonged to other Hungarian ISPs. While these incidents were quite small in scale, they could have been attempts to conduct censorship by using the BGP routing system.

January 2019[20]
Amidst the demonstrations in Zimbabwe due to rising fuel prices, the government was accused of blocking networks like WhatsApp and Facebook. It was also accused of unfairly using BGP routing to cause Internet shutdowns. While there are no reported incidents, there was a number of prefix outages on those days.

June 2019[21]
Due to a leak Verizon did not filter, this important American Internet provider ended up rerouting a large portion of the traffic to a small company in Pennsylvania. This led to service disruption and service degradation in the access to different sites and services. Cloudflare was one of the most affected parties, which resulted in even more Internet sites being knocked offline.

---

7 ‹https://www.bgp.us/case-studies/›
8 ‹https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/›
9 ‹https://arstechnica.com/information-technology/2015/07/hacking-team-orchestrated-brazen-bgp-hack-to-hijack-ips-it-didnt-own/›
10 Ídem.
11 ‹https://dyn.com/blog/why-the-internet-broke-today/›
12 ‹https://twitter.com/bgpmon/status/846087079763177472›
13 ‹https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/›
14 ‹https://www.internetsociety.org/blog/2017/08/google-leaked-prefixes-knocked-japan-off-internet/›
15 ‹https://bgpmon.net/todays-bgp-leak-in-brazil/›
16 ‹https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/›
17 ‹https://www.internetsociety.org/blog/2017/12/another-bgp-routing-incident-highlights-internet-without-checkpoints/›
18 ‹https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/›
19 ‹https://blog.talosintelligence.com/2018/11/persian-stalker.html›
20 ‹https://www.thesouthafrican.com/news/zimbabwe-protest-mnangagwa-accused-blocking-whatsapp-facebook/›
21 ‹https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/›

Event Analysis

The incidents listed in this report's timeline are just the tip of the iceberg. They are only some of the events that attracted the most attention and affected a large amount of Internet users for a considerable amount of time or under a critical social context. However, most incidents go generally unnoticed. This report analyzes the entirety of the events to better understand the situation of routing security in the world and in our region.

Methodology

As explained, there are two types of BGP incidents: route leaks and hijacks. This report analyzes the events collected by the Bgpstream.com portal, which also registers another type of event: outages. These happen when an autonomous system stops announcing certain prefixes. From this source, we analyzed the events registered in 2017, 2018 and part of 2019.

Autonomous systems may be involved in different ways in each event. When it comes to leaks, there is someone who effectively *leaks* a route that they must not publish (the culprit), and there is the route leading to a prefix that belongs to some other AS (the affected party or victim). Additionally, the leak is transmitted to other autonomous systems that accept such route due to poor filtering policies (propagators).

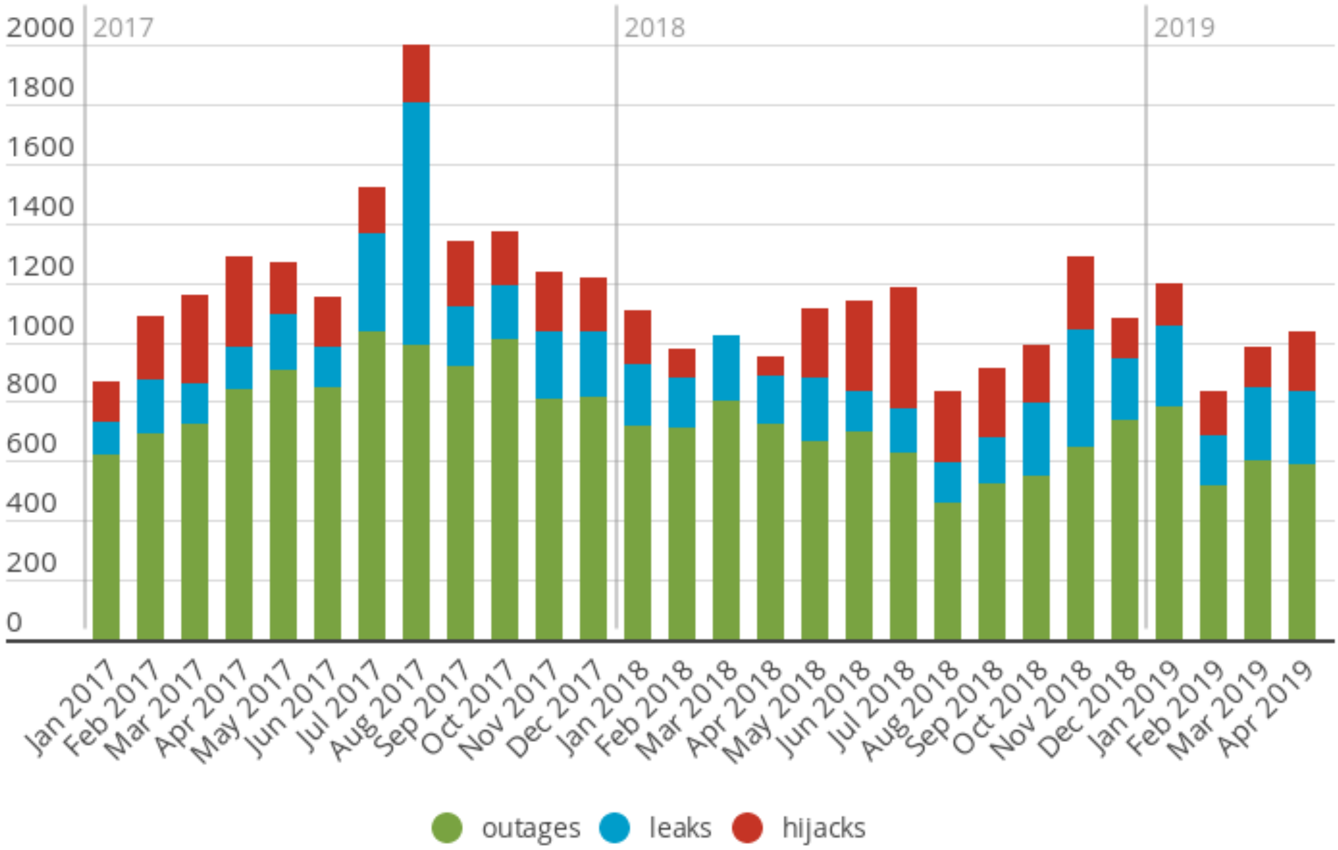
As regards route hijacks, there is the AS fraudulently announcing a prefix that does not belong to it (the culprit) and the AS that actually has such prefix (the affected party or victim). In both cases, the autonomous systems that observe these events can also be registered, but this information is not analyzed, since they are not actively involved in the incidents.

In order to associate autonomous systems to territories, we first take the estimate made by BGPSTREAM, which uses the MaxMind's GeoLite City database. If this query does not give an appropriate result or if it has not been made, it is associated to the country each RIR associates to it when it is registered. While its prefixes do not always end up being configured in devices that are based in such territory, it is still a good estimate to use these registries to associate autonomous systems to countries and, on the basis of such association, to generate statistics at the geographical level.

Numbers around the World

Each day, the BGP tables of tens of thousands of autonomous systems change and announce different routes. Graph 1 shows the number of incidents that happened between 2017 and April 2019 registered by BGP Stream.

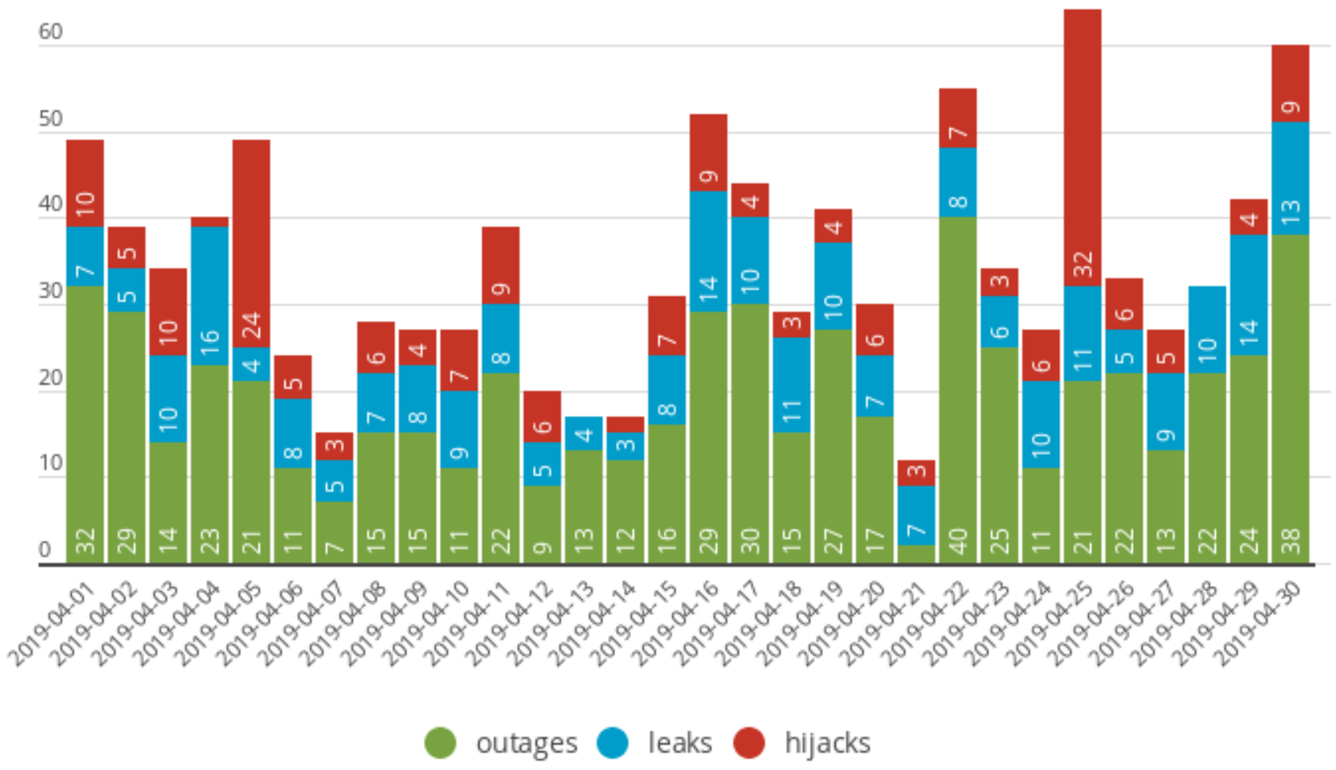
Graph 1: Number of incidents by month around the world.



Source: ‹https://bgpstream.com›

Let us remember that an event is not necessarily a deliberate attack, since some announcements may be misinterpreted and cause false positives, or they may be the result of configuration errors (i.e., unintentional). On the other hand, as mentioned above, there are BGP incidents on the network every day, even if they do not have a big impact or they are not newsworthy. We can see this, for example, when we look at April of 2019, with day-to-day details on the incidents that took place.

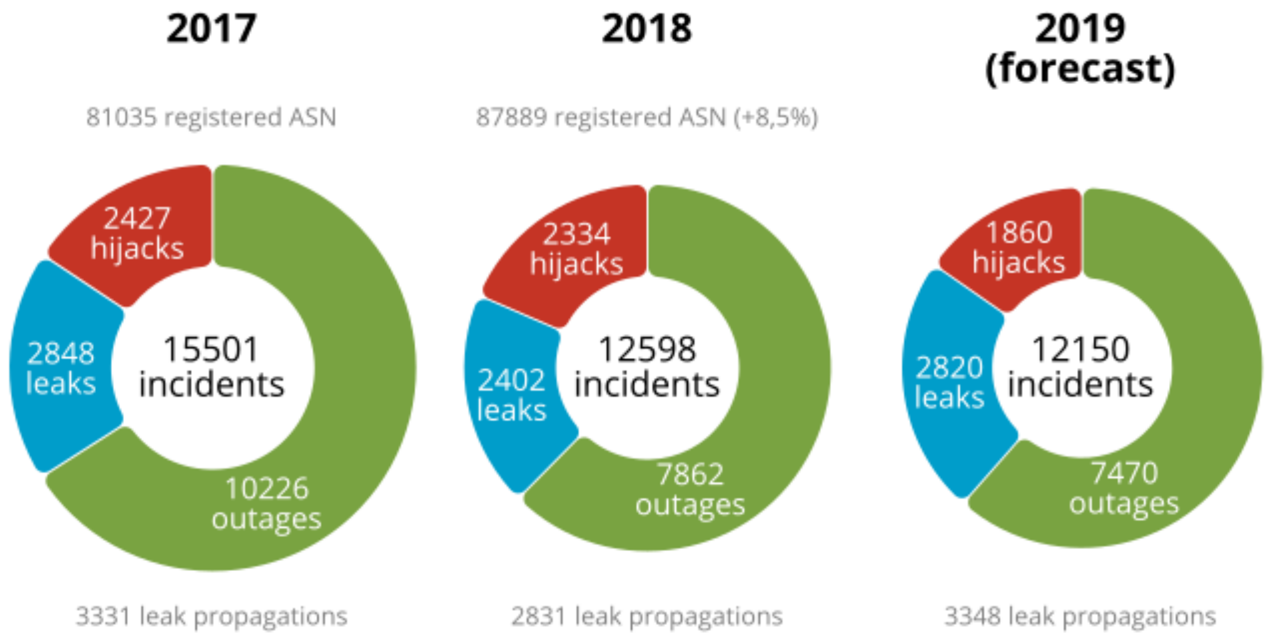
Graph 2: Number of incidents occurred each day around the world in April 2019.



Source:‹https://bgpstream.com›

At first, it may seem that the number of incidents is constant. However, there is a downward trend in the following graph, where we can see the number of incidents classified by year and type (below, the graph also shows the number of propagations; i.e., when an autonomous system propagates a leak because it did not implement the appropriate filtering policies).

Graph 3: Number of incidents by year at the global level.



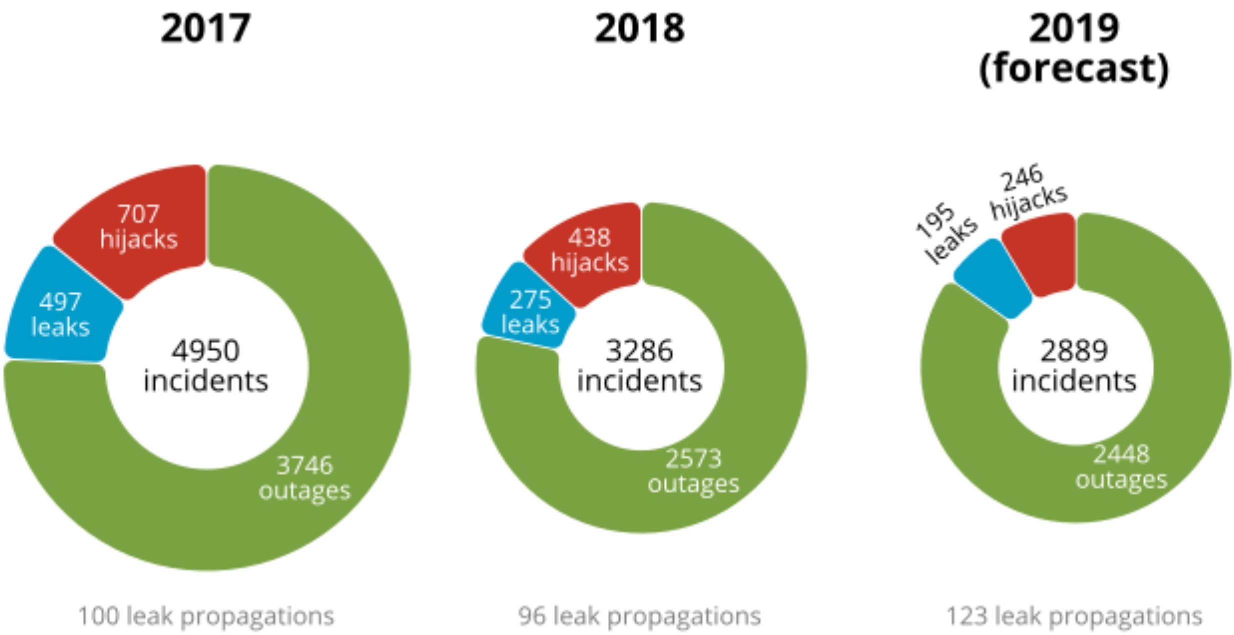
Note: The 2019 forecast was made based on the 4050 events registered until April of that year.
Source: https://bgpstream.com https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html

Along with the decline of the annual total amounts, we must take into account that there are more and more autonomous systems being registered and connected to the network. The year 2017 ended with 81,035 registered ASNs around the world, while 2018 ended with 87,889 registered ASNs. There was an 8.5% increase, akin to the one expected for 2019 (it is expected that 94,000 ASNs will be registered by the end of 2019).

While the decline in the number of annual incidents may seem small, we can infer that it is a significant improvement considering the number of autonomous systems has increased. This may be due to the adoption of new filtering measures in BGP routing tables, like the MANRS proposal by the Internet Society, an initiative that will be explained in detail later on. Among these measures, there is also a larger number of operators implementing RPKI.

When carrying out the same analysis narrowing the study down to incidents involving countries in Latin America and the Caribbean, the improvement from 2017 to 2018 is even more pronounced.

Graph 4: Number of incidents by year in Latin America and the Caribbean.



Note: The 2019 forecast was made based on the 963 events registered until April of that year.
Source: ‹https://bgpstream.com› and ‹https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html›

When it comes to specific autonomous systems, we can rank every case in order to know which are the ones that are most involved in these events.

Table 1: World's top 5 autonomous systems (2017 and 2018) that caused the highest number of leaks.

2017			2018		
ASN	**Description**	**Leaks**	**ASN**	**Description**	**Leaks**
4258	atg-4258 - accretive networks, us	51	3910	centurylink-europe-legacy-qwest - centurylink Communications, LLC, US	337
393861	inova-primaryasn-01 - inova health system foundation, us	45	5391	T-ht croatian telecom inc., hr	134
7991	centurylink-legacy-savvis-asia-transit - centurylink communications, llc, us	40	58601	aamra-atl-bd aamra technologies limited, bd	115
24990	equinix-fr-asn equinix france autonomous system, fr	39	7991	centurylink-legacy-savvis-asia-transit - centurylink communications, llc, us	86
3908	centurylink-asia-legacy-qwest - centurylink communications, llc, us	29	39386	stc-igw-as, sa	45
37452	cb-nigeria, ng	29			
32787	prolexic-technologies-ddos-mitigation-network - akamai technologies, inc., us	29			

Source: ‹https://bgpstream.com›

Table 2: World's top 5 autonomous systems (2017 and 2018) that were the most affected by leaks.

2017			2018		
ASN	Description	Leaks	ASN	Description	Leaks
27066	dnic-asblk-27032-27159 - dod Network Information center, US	15	18399	ytcl-as-ap yatanarpon teleport company limited, mm	21
63852	Fmg-mm myanmar net, mm	15	27066	dnic-asblk-27032-27159 - dod network information center, us	19
1541	dnic-asblk-01534-01546 - headquarters, usaisc, us	13	1541	dnic-asblk-01534-01546 - headquarters, usaisc, us	18
13896	Thinkingphones - fuze inc, us	12	59209	whil-bd walton hi-tech industries ltd, bd	15
38456	Speedcast-au speedcast australia pty limited, au	12	14210	edgecast-dca - mci communications services, inc. d/b/a verizon business, us	14

Source:‹https://bgpstream.com›

Table 3: World's top 5 autonomous systems (2017 and 2018) that caused the highest number of hijacks.

2017			2018		
ASN	Description	Hijacks	ASN	Description	Hijacks
49291	interpro-as, ru	90	50607	epix-kgm, pl	158
198949	vs-as, il	53	37468	angola-cables, ao	131
263444	open x tecnologia ltda, br	50	198726	komdsl, de	75
39523	dv-link-as, ru	29	8859	osn bucher str. 78, de	37
27884	cablecolor s.a., hn	25	399261	bogon as - iana unallocated asn, zz	33

Source:‹https://bgpstream.com›

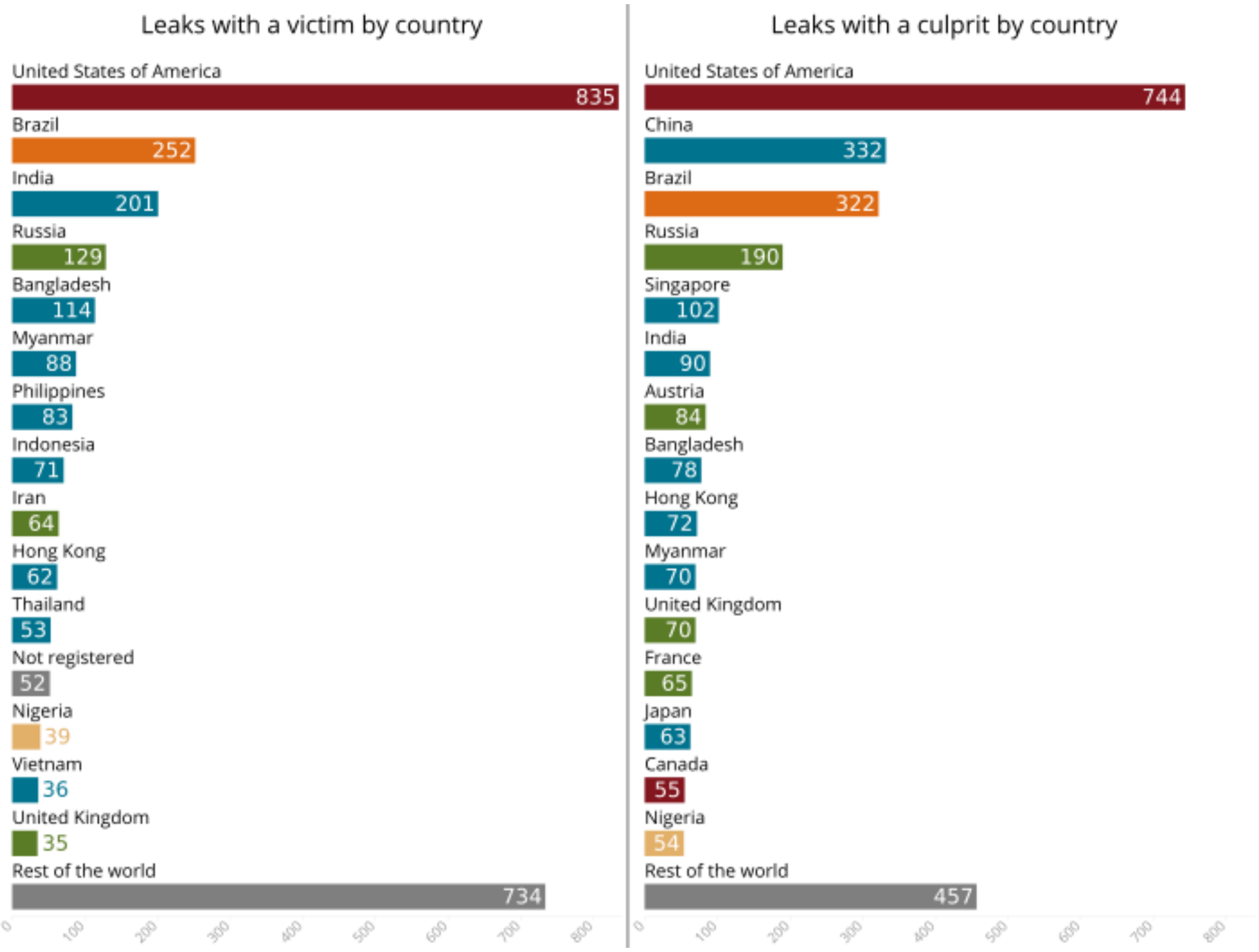
Table 4: World's top 5 autonomous systems (2017 and 2018) that were the most affected by hijacks.

2017			2018		
ASN	Description	Hijacks	ASN	Description	Hijacks
13489	epm telecomunicaciones s.a. e.s.p., co	233	14259	gtd internet s.a., cl	79
21928	t-mobile-as21928 - t-mobile usa, inc., us	17	35916	multa-asn1 - multacom corporation, us	15
35994	akamai-as - akamai technologies, inc., us	16	25577	c4l-as, gb	15
203661	william, gb	12	35994	akamai-as - akamai technologies, inc., us	14
1200	ams-ix1, nl	12	21928	t-mobile-as21928 - t-mobile usa, inc., us	14

Source: ‹https://bgpstream.com›

We can see that the majority of autonomous systems in the tables belong to the USA. Is this a rule? What countries are the most involved in routing incidents? To answer these questions, we can analyze the data by country. Let us start with the 2017 leaks.

Graph 5: BGP leaks in 2017 by country.

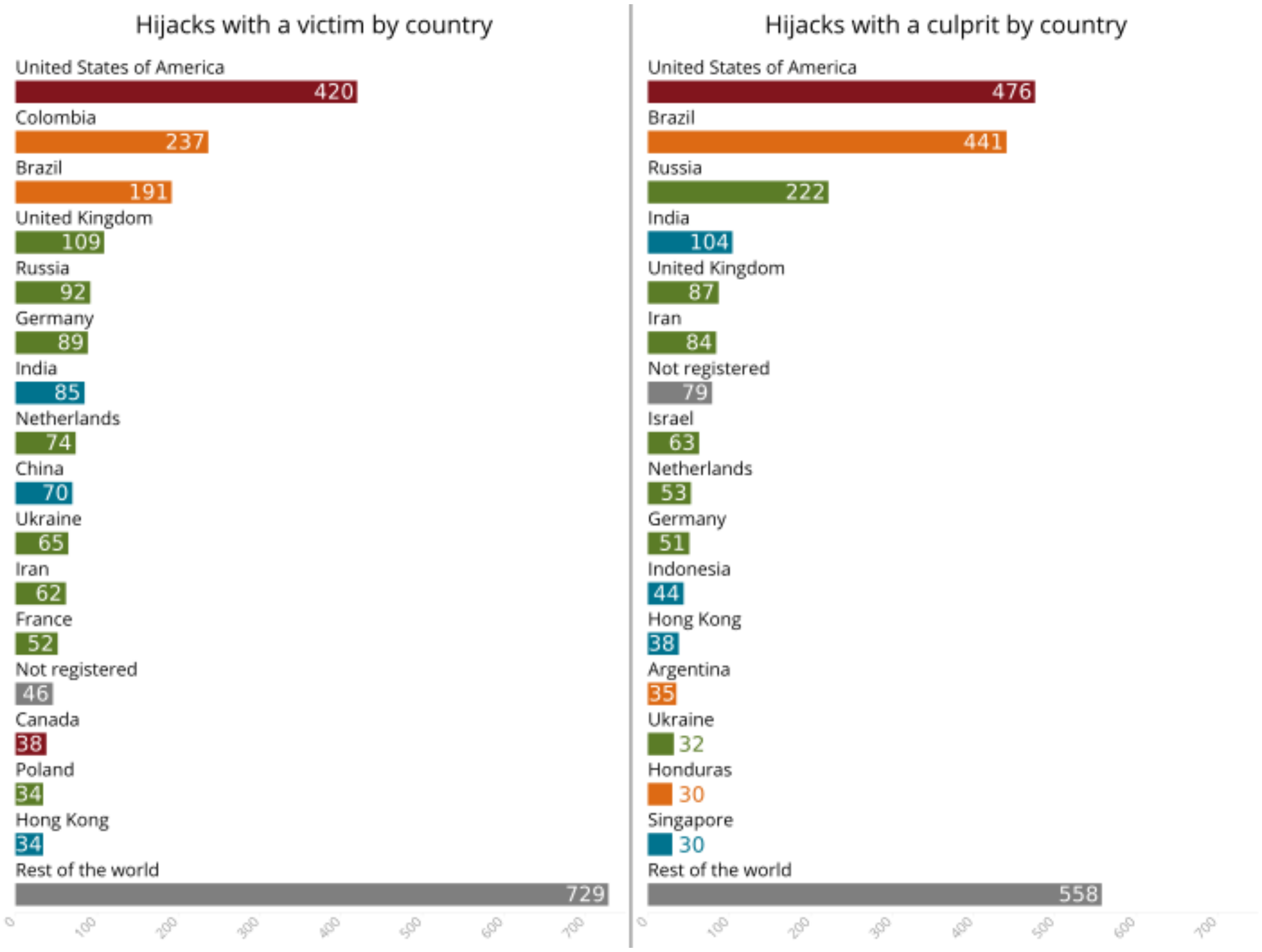


Source: ‹https://bgpstream.com›

Graph 5 groups the number of incidents according to the countries in which there were AS's involved. They are grouped according to the part they played in the leak: either as "culprits", which announce a route out of their desired scope or as "victims", whose IP prefixes were wrongly announced.

As we can see, there is a significant predominance of USA in all cases. This was foreseeable, since this country not only has a huge number of service providers, but also hosts all the companies that play important roles in the Internet ecosystem. As regards Latin America, only Brazil got to be in these rankings, which also makes sense, as it is the second country with the largest number of connected autonomous systems. What about route hijacks?

Graph 6: BGP hijacks in 2017 by country.



Source: ‹https://bgpstream.com›

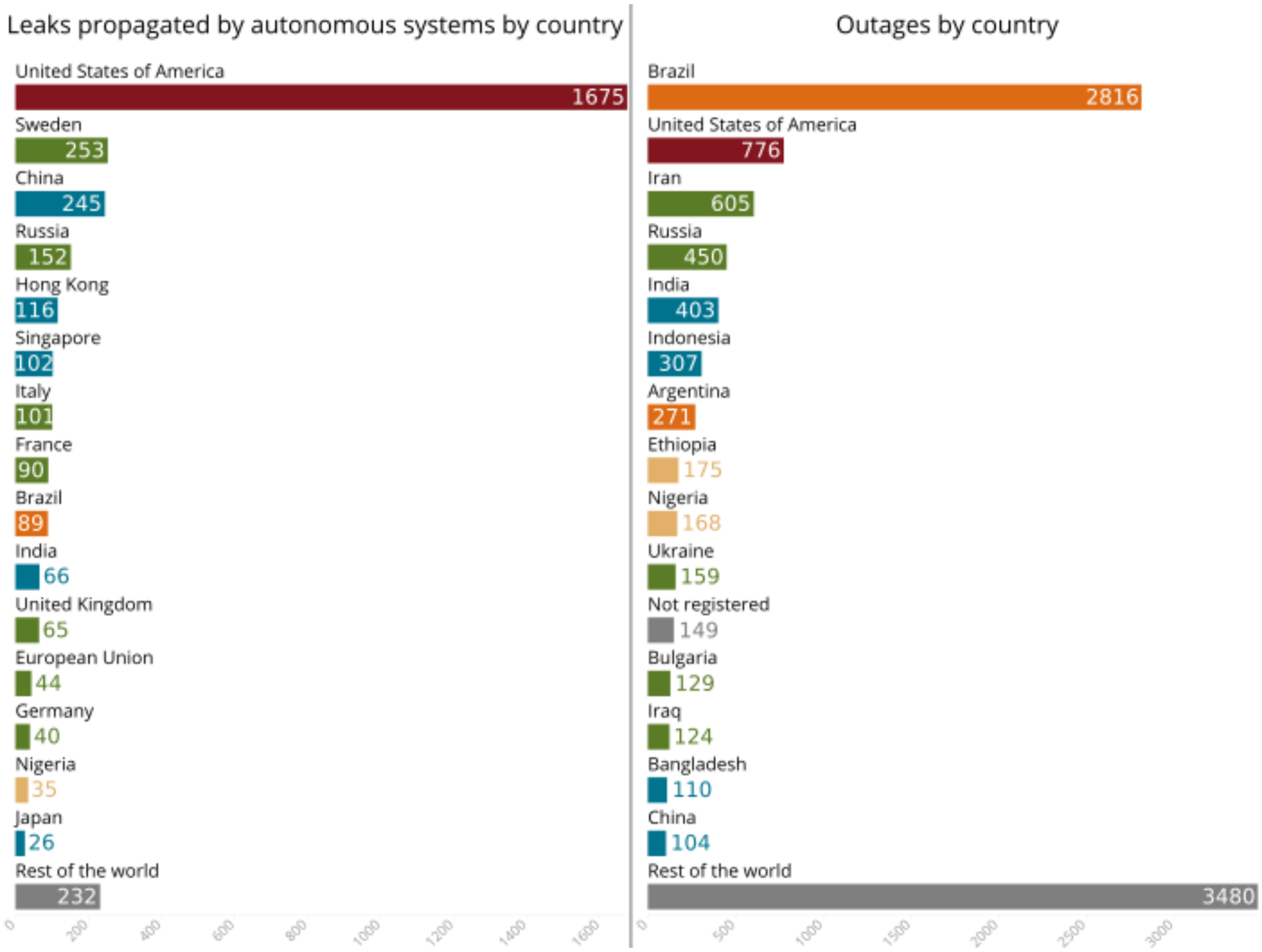
Graph 6 shows that Brazil had almost the same number of autonomous systems responsible for hijacks as the USA. According to the timeline in this report, there were repeated routing incidents in Brazil in 2017, which can also be seen in the quantitative statistics. Other countries in the region, like Argentina and Honduras, also made it to this ranking.

Colombia's position is noteworthy. It is the second country with the largest amount of autonomous systems that had their prefixes fraudulently announced by others. If we look at a differentiated ranking grouped by ASNs, AS13489, registered in Colombia, was the most affected victim of fraudulent prefix announcements that year. When analyzing the announcements made by this autonomous system that year, we reach the conclusion that these incidents are not hijacks, but events caused by a configuration error in that particular AS.

During 2017, this autonomous system announced that it owned the whole 2800::/12 IPv6 prefix. This is the block assigned to LACNIC by IANA, which is distributed into smaller prefixes for all the operators in our region that request IPv6 addresses. For some reason —probably a wrong configuration—, AS13489 had been announcing the entire prefix, together with the ones that it actually has. So, every time another operator in the region started to announce its new IPv6 prefixes via its ASNs, BGPSTREAM interpreted it as a hijack attempt (since one of the ways of winning a route against an ASN is by announcing a more specific prefix). While this incident is not a route hijack, it shows that there is little control in the BGP and that it is sensitive to operator errors.

Finally, we can also analyze two other facts from 2017, registered by BGPSTREAM: outages (incidents in which an AS stops announcing IP prefixes that belong to it, making them inaccessible) and detected BGP leak propagations (incidents in which an AS gets a route due to a leak and, having inadequate filtering policies, it continues propagating that route to other autonomous systems).

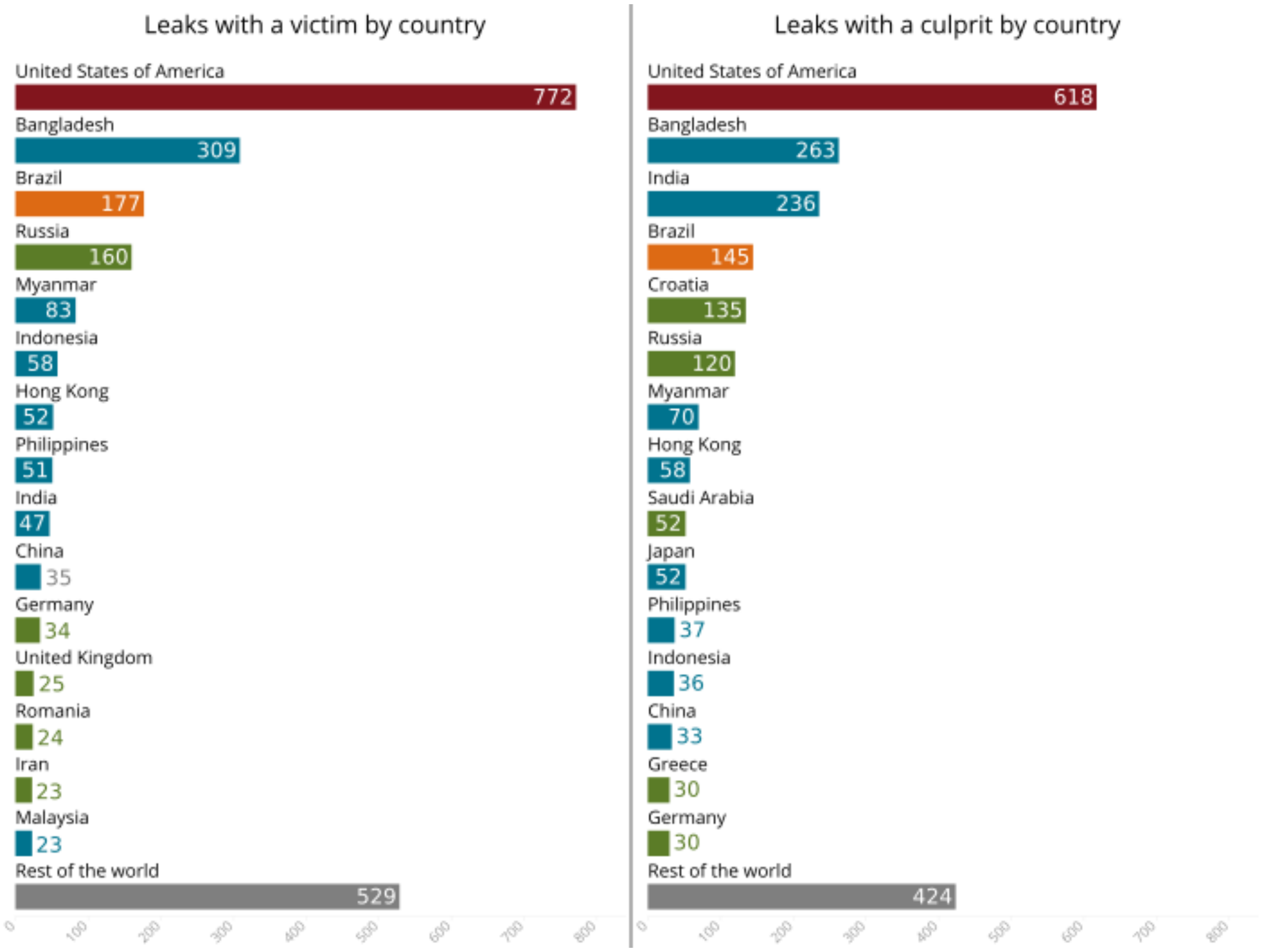
Graph 7: Outages and BGP leak propagations in 2017 by country.



Source:‹https://bgpstream.com›

Graph 7 shows that the United States has an unresolved issue when it comes to leak propagations. This country caused more than half of the leaks in 2017. Additionally, we can see the excessive number of outages in Brazil for that year. How did 2018 look like?

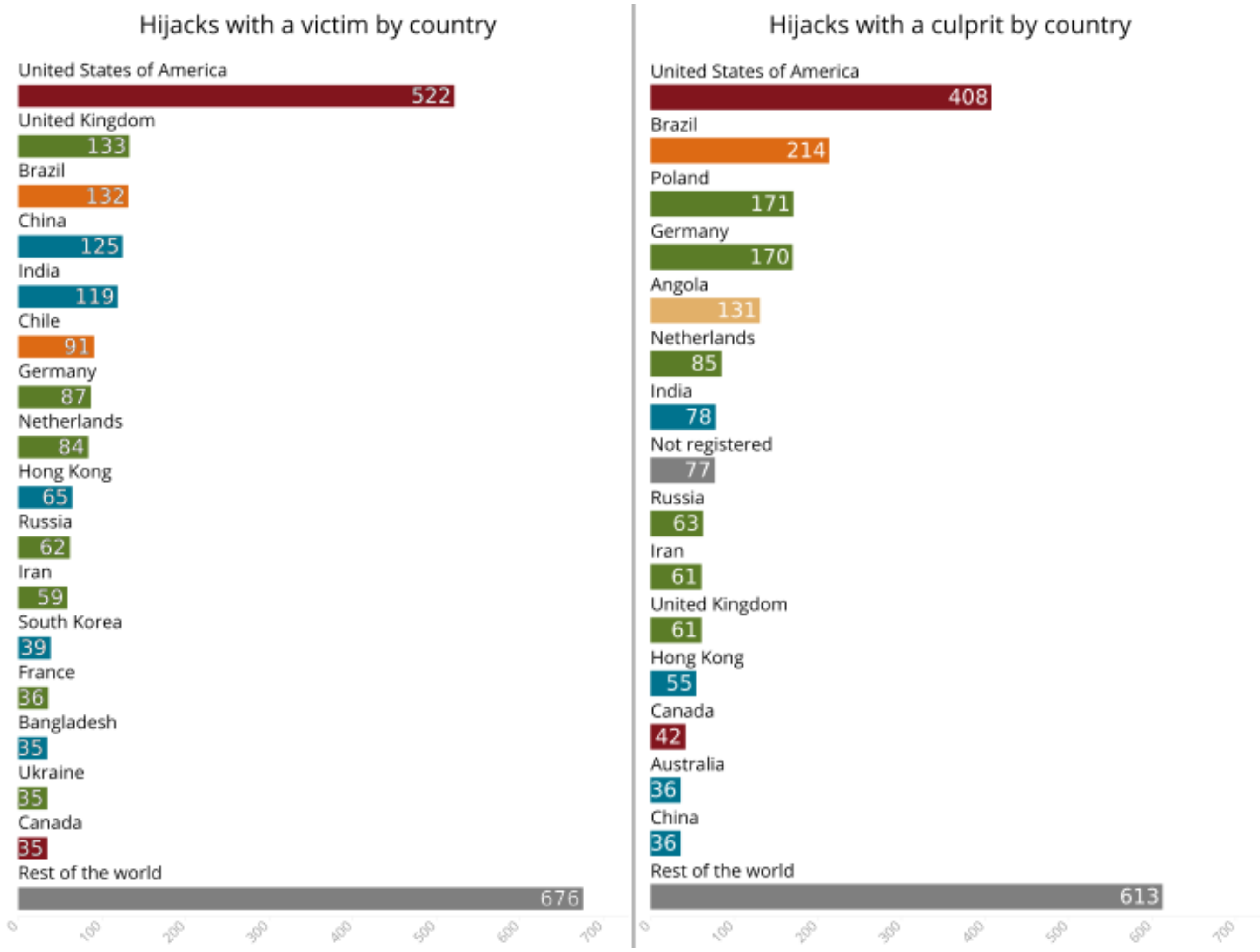
Graph 8: BGP leaks in 2018 by country.



Source: ‹https://bgpstream.com›

Graph 8 allows us to see how the number of the incidents has dropped in general terms, except for some specific cases like Bangladesh. The United States is still the country with the largest number of leaks. While Brazil is still among the top countries, it has gone down one position in both rankings. Countries in Asia and the Pacific continue to be predominant.

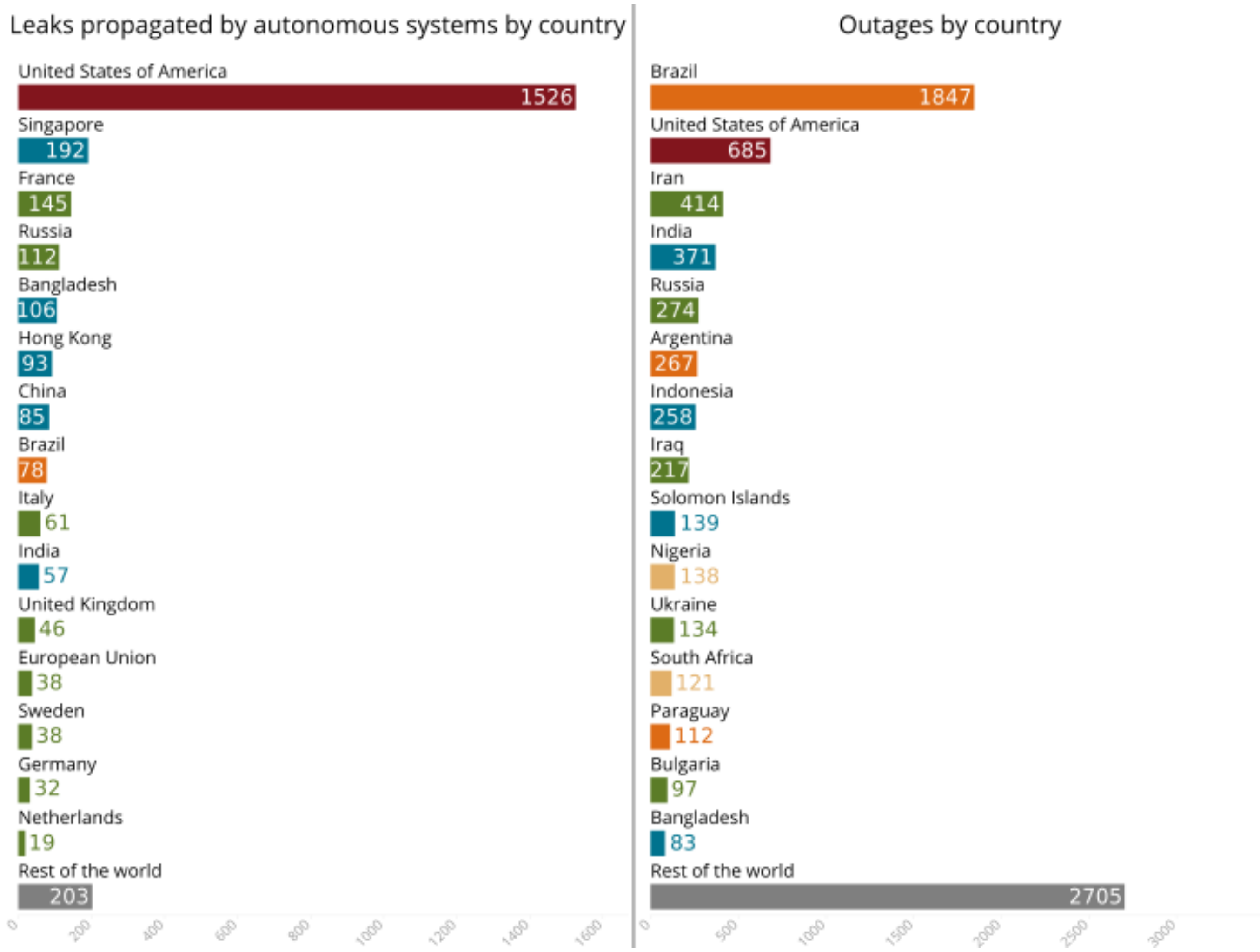
Graph 9: BGP hijacks in 2018 by country.



Source: ‹https://bgpstream.com›

Graph 9 shows that there is not a big difference as regards hijacks. It is worth noting that, while Brazil is still in the second position as to the highest number of autonomous systems that fraudulently announced prefixes, the number of incidents in the country has relatively been cut in half (from 18.27% to 9.16%). Additionally, there are no Latin American countries among the top 15 countries with the highest number of incidents this year. Finally, we analyze the outages and leak propagations in 2018.

Graph 10: Outages and BGP leak propagations in 2018 by country.



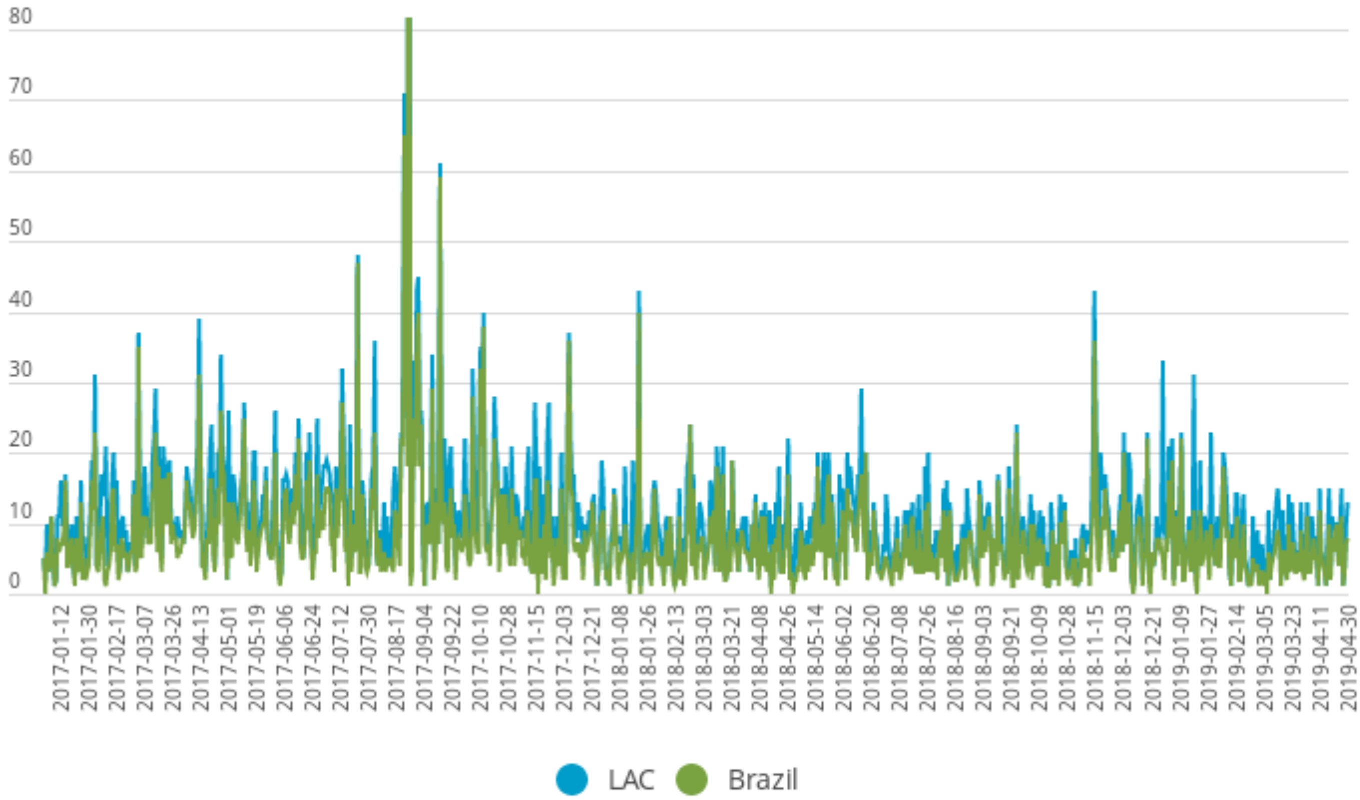
Source:‹https://bgpstream.com›

Graph 10 does not show many differences for 2018 when it comes to outages and leak propagations. While Brazil's outages have been cut in half, it remains in the first place. Other countries from our region made it to this ranking, like Argentina and Paraguay.

Numbers in the Region

It is important to carry out a similar analysis for the countries in Latin America and the Caribbean to understand the region's situation when compared to the rest of the world. We need to take into consideration one particular fact: the size of Brazil. When looking at numbers from all around the world, we can see that Brazil is always among the top five countries with autonomous systems involved in different routing incidents. In addition to this, out of the 4950 BGP incidents in Latin America and the Caribbean in 2017, 3768 involved some ASN from Brazil (76.1%). In 2018, Brazil was involved in 2363 out of 3286 incidents in the region (71.9%).

Graph 11: Incidents in Latin America and the Caribbean vs. Incidents in Brazil.



Source: ‹https://bgpstream.com›

We can see that the line indicating the events that occurred across Latin America is just above the one representing the events that occurred only in Brazil. This means that the events occurring in other countries of the region are overshadowed by a great activity coming from just one single country.

Events by Country

While Brazil ends up shaping the general statistics when analyzing the whole region, it is still worth looking into other Latin American countries individually. Thus, in order to take a quick glance at the routing situation in each country, table 5 provides a list of events grouped by country, for 2017:

Table 5: Number of incidents by country in Latin America and the Caribbean (2017).

Country / Region		Leaks (c)	Leaks (v)	Leaks (a)	Hijacks (c)	Hijacks (v)	Total	ASNs	Total/ASNs
AR	Argentina	0	11	0	35	18	64	600	0.11
BZ	Belize	0	0	0	2	2	4	10	0.4
BO	Bolivia	0	3	0	3	2	8	25	0.32
BR	Brazil	322	252	89	441	191	1295	4939	0.26
CL	Chile	1	1	1	4	30	37	176	0.21
CO	Colombia	0	2	7	9	237	255	114	2.24
CR	Costa Rica	6	8	0	2	5	21	58	0.36
EC	Ecuador	2	3	2	7	8	22	67	0.33
GT	Guatemala	0	2	0	4	9	15	33	0.45
HN	Honduras	0	0	0	30	5	35	59	0.59
JM	Jamaica	0	0	0	5	0	5	8	0.63
MX	Mexico	4	9	1	1	4	19	233	0.08
NI	Nicaragua	0	1	0	5	4	10	21	0.48
PA	Panama	0	2	0	3	2	7	77	0.09
PE	Peru	0	0	0	2	4	6	28	0.21
PR	Puerto Rico	5	4	0	5	0	14	48	0.29
BL	Saint Barthélemy	0	1	0	1	0	2	3	0.67
MF	Saint Martin (FR)	0	1	0	3	0	4	3	1.33
TT	Trinidad and Tobago	0	1	0	2	1	4	13	0.31
VI	Virgin Islands (US)	0	2	0	1	2	5	6	0.83
VE	Venezuela	6	12	0	1	1	20	53	0.38
	Rest of lac countries	3	4	0	5	6	18	190	0.09
	lac total	349	319	100	571	531	1870	6764	0.28
	World total	2848	2848	3331	2427	2427	13881	80866	0.17
US	United States	744	835	1675	476	420	4150	16379	0.25

Source: ‹https://bgpstream.com› ripe ncc

References:

- Leaks (c): Number of autonomous systems that caused a leak.
- Leaks (v): Number of autonomous systems whose prefixes were leaked by another AS.
- Leaks (a): Number of autonomous systems that accepted a leak.
- Hijacks (c): Number of autonomous systems that fraudulently announced a prefix.
- Hijacks (v): Number of autonomous systems that were victims of a hijack.
- Total: Overall number of recorded events.
- ASNs: Number of ASNs that were active in the country by the end of the year. Source: ‹https://stat.ripe.net/›
- Total/ASNs: Division resulting from both values.

This table includes countries where at least five incidents occurred in 2017 or 2018. The rest of them are grouped into "Rest of LAC countries" and they are: Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Bonaire, Saint Eustatius and Saba, Bouvet Island, British Virgin Islands, Cayman Islands, Cuba, Curaçao, Dominica, Dominican Republic, El Salvador, Falkland Islands, French Guiana, Grenada, Guadeloupe, Guyana, Haiti, Martinique, Montserrat, Paraguay, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, St. Martin's Dutch side, South Georgia and the Sandwich Islands, Suriname, Turks and Caicos Islands, and Uruguay. For the purposes of comparison, we have also grouped Latin America (overall), the whole world, and the United States.

Comparing the absolute number of the amount of events is not very enriching, since countries vary in size in many respects: territory, population, connected users, registered autonomous systems. This is why — in the pursuit of the harmonization of statistics— the table includes the number of autonomous system each country has, so that the number of incidents can later be divided by that value, resulting in values that can be compared. Moreover, such value can be compared year over year. The following is a table like the previous one for 2018:

Table 6: Number of incidents by country in Latin America and the Caribbean (2018).

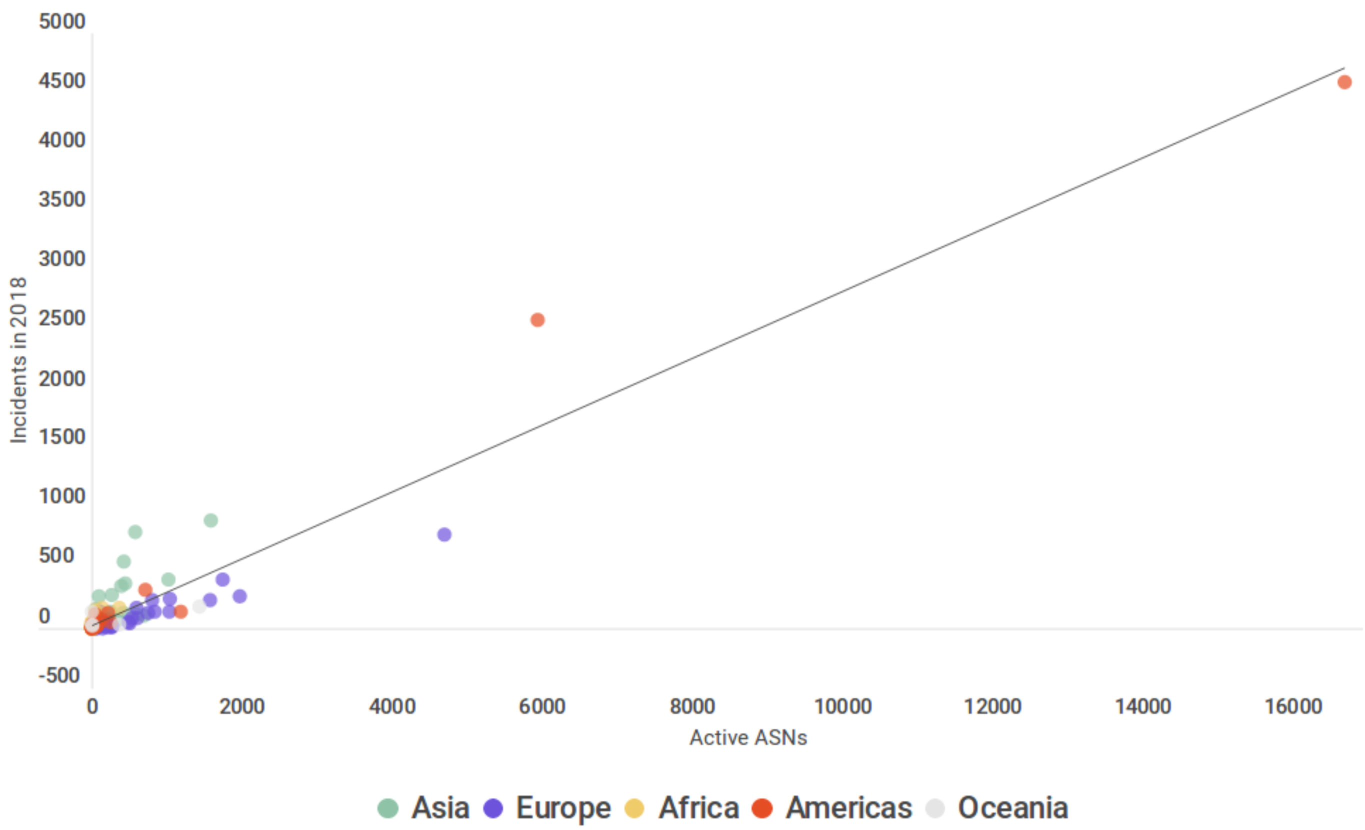
Country / Region		Leaks (c)	Leaks (v)	Leaks (a)	Hijacks (c)	Hijacks (v)	Total	ASNs	Total/ASNs
AR	Argentina	1	8	1	21	18	49	718	0.07 (-0.04)
BZ	Belize	1	2	0	2	1	6	17	0.35 (-0.05)
BO	Bolivia	0	0	0	1	0	1	30	0.03 (-0.29)
BR	Brazil	145	177	78	214	132	746	5942	0.13 (-0.13)
CL	Chile	0	2	0	10	91	103	219	0.47 (0.26)
CO	Colombia	17	3	0	15	8	43	127	0.34 (-1.9)
CR	Costa Rica	6	7	0	3	3	19	67	0.28 (-0.08)
EC	Ecuador	0	1	0	7	7	15	90	0.17 (-0.16)
GT	Guatemala	0	0	1	0	8	9	36	0.25 (-0.2)
HN	Honduras	0	0	0	9	8	17	62	0.27 (-0.32)
JM	Jamaica	0	0	0	2	1	3	8	0.38 (-0.25)
MX	Mexico	3	3	2	4	4	16	250	0.06 (-0.02)
NI	Nicaragua	0	0	0	6	0	6	21	0.29 (-0.19)
PA	Panama	2	3	14	8	3	30	76	0.39 (+0.3)
PE	Peru	0	0	0	4	3	7	31	0.23 (+0.02)
PR	Puerto Rico	0	1	0	4	3	8	49	0.16 (-0.13)
BL	Saint Barthélemy	0	5	0	0	0	5	3	1.67 (+1)
MF	Saint Martin (FR)	0	0	0	0	0	0	4	0 (-1.33)
TT	Trinidad and Tobago	0	2	0	2	1	5	14	0.36 (+0.05)
VI	Virgin Islands (US)	0	0	0	0	1	1	6	0.17 (-0.66)
VE	Venezuela	0	1	0	2	1	4	54	0.07 (-0.31)
	Rest of LAC countries	0	3	0	6	8	17	219	0.08 (-0.01)
	LAC total	175	218	96	320	301	1110	8043	0.14 (-0.14)
	World total	2402	2402	2831	2335	2335	12305	87853	0.14 (-0.03)
US	United States	681	772	1526	408	522	3909	16689	0.23 (-0.02)

Source:‹https://bgpstream.com› ripe ncc

At first glance, we can see that the relation between the number of incidents and the number of autonomous systems decreased in most of the countries of the region and also around the world.

This metric, which stems from dividing the total number of incidents by the number of active ASNs by country, seems appropriate when comparing different countries, leaving behind the size bias. This can be verified when looking at the correlation between both values. If we take the 2018 statistics, they result in a correlation coefficient of 0.95; i.e., a strong correlation.

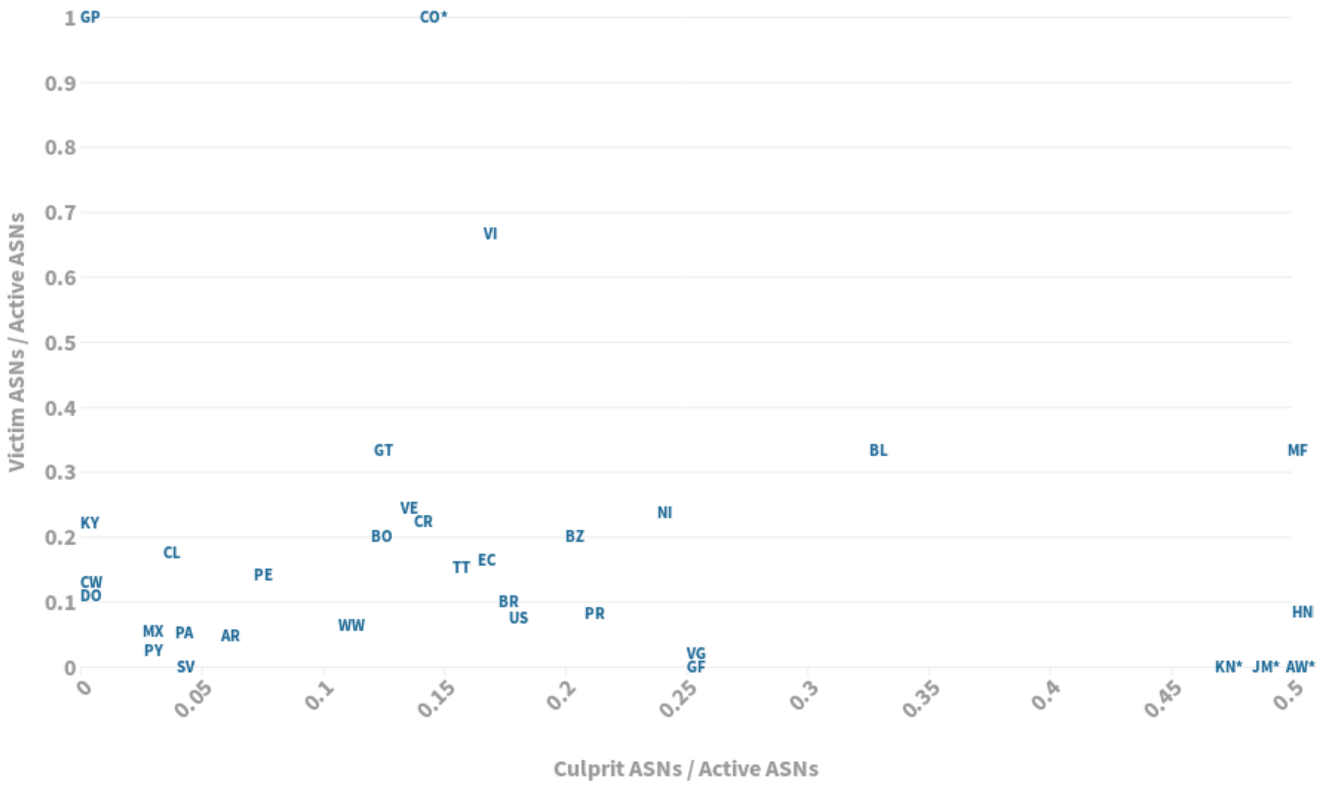
Graph 12: Number of incidents by country vs. Number of active autonomous systems (2018).



Source: ‹https://bgpstream.com› ripe ncc

We can also compare countries, as in the following graph —where different countries in the region are compared, along with the United States (US) and the world total (WW). In order to make this comparison, on the vertical axis we use a metric that consists in adding, by country, the events in which an autonomous system fell victim either to a hijack or leak, and dividing that by the number of active ASNs at the end of that year. On the horizontal axis, the metric is the number of autonomous systems responsible for incidents by country (leaks or leak propagation and hijacks), divided by the number of active autonomous systems at the end of that year.

Graph 13: Comparison between LAC countries based on 2017 incidents.



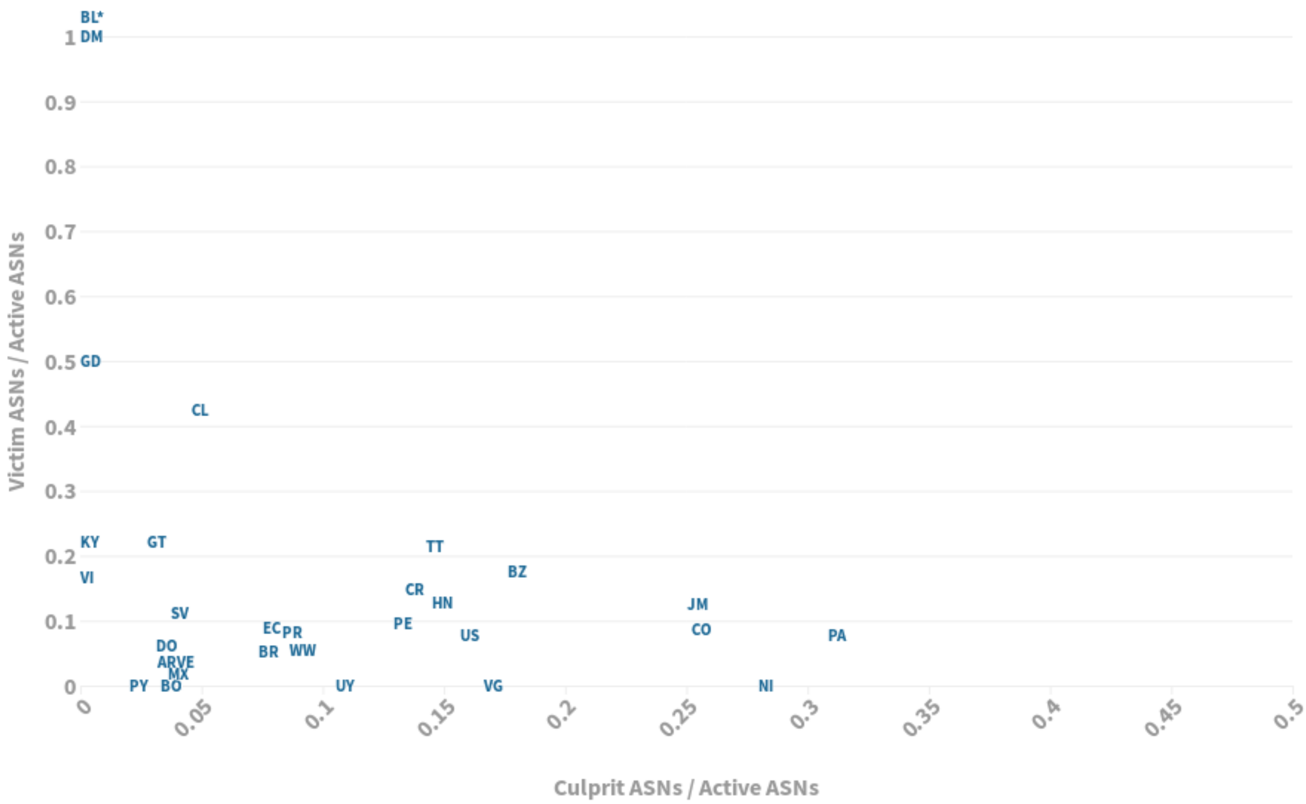
Source:‹https://bgpstream.com› ripe ncc

Countries outside the graph limits:

- Colombia (CO): Victim ASNs / Active ASNs: 2.1
- Saint Kitts and Nevis (KN): Culprit ASNs / Active ASNs: 1
- Jamaica (JM): Culprit ASNs / Active ASNs: 0.6
- Aruba (AW): Culprit ASNs / Active ASNs: 3

Countries that are closer to the origin [0.0] are better positioned and have a smaller number of autonomous systems as protagonists of routing incidents. We can see that there is a group of countries (Argentina, Chile, Mexico, Panama and Peru, among others) that is in a better situation than the global average. Brazil is in a situation akin to the one of the United States. Countries in Central America and Islands in the Caribbean arrived at an average of ASN incidents that was higher than the global average.

Graph 14: Comparison between LAC countries based on 2018 incidents.



Source: ‹https://bgpstream.com› ripe ncc

Countries outside the graph limits:

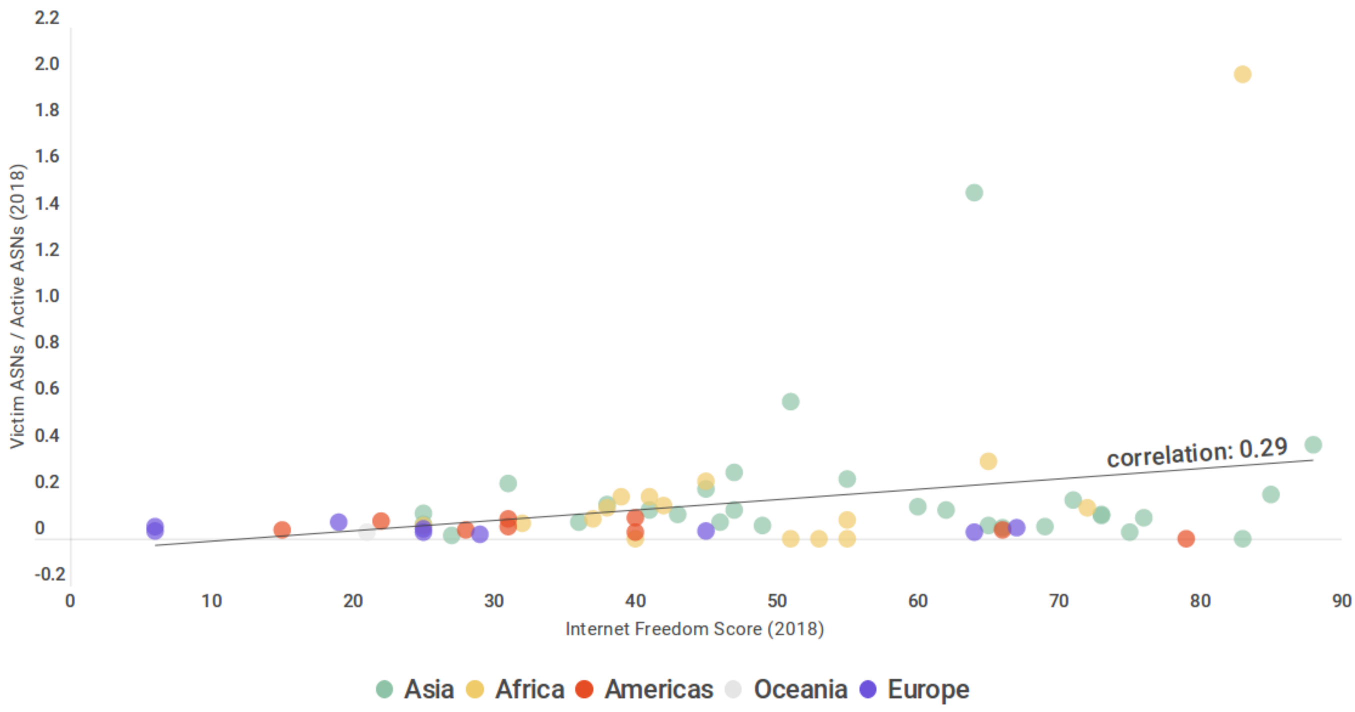
- Saint Barthélemy (BL): Victim ASNs / Active ASNs: 1.7

Brazil's situation improved substantially in 2018, reaching a position below the global average. In general terms, countries improved their statistics this year and came closer to the origin in the graph, but most of the countries in Central America are still above the average as regards the number of incidents.

Apart from comparing countries or their evolution throughout the years, this metric —which counts incidents and divides them by the number of active ASNs by country— can also be used to search for correlations with other metrics and indicators of the countries. For instance, there is a slight correlation between the amount of victim ASNs by country and the Freedom of the Net Index published by Freedom House.[22] This index measures each country's level of Internet and digital media freedom. It is based on a set of methodology questions —developed in consultation with international experts— to capture the vast array of relevant issues that enable Internet freedom. The methodology includes 21 questions and nearly 100 subquestions, divided into three categories: Obstacles to Access, Limits on Content and Violations of User Rights.

[22] ‹https://freedomhouse.org/report/freedom-net/freedom-net-2018›

Graph 15: Correlation between victim ASNs by country and Freedom of the Net Index.



Source:‹https://bgpstream.com› / ripe ncc / ‹https://freedomhouse.org/report/countries-net-freedom-2018›

The correlation is not very strong, but having analyzed specific cases like the ones in this report, we can infer that, if the Internet has a weak routing infrastructure, it becomes prone to curtailing freedoms.

Rankings in Latin America

Just like at the global level, these are the top 5 autonomous systems that were the most involved in routing incidents within our region.

Table 7: LAC autonomous systems that caused the highest number of leaks.

2017			2018		
ASN	Description	Leaks	ASN	Description	Leaks
266430	VICTOR.NET E LINK EVOLUTION TELECOM LTDA ME, BR	19	52654	BI-LINK TELECOM, BR	33
52866	IVELOZ TELECOM SERV. EM TELECOMUNICACOES LTDA, BR	16	61678	NETWAY INFORMATICA LTDA, BR	17
262740	VELOO NET LTDA, BR	10	263798	UFINET COLOMBIA, S. A., CO	12
16735	ALGAR TELECOM S/A, BR	6	61832	FORTEL FORTALEZA TELECOMUNICACOES LTDA, BR	8
27908	TRACITY INC., CR	6	52865	R. JOSE DA SILVA E CIA LTDA - ONDAÁGIL, BR	8
			28327	PS5 INTERNET, BR	8

Source: ‹https://bgpstream.com›

Table 8: LAC autonomous systems that were the most affected by leaks.

2017			2018		
ASN	Description	Leaks	ASN	Description	Leaks
263935	URUCUINET TELECOM E INFORMATICA LTDA - ME, BR	5	264043	SILFERNET COMÉRCIO E SERVIÇOS LTDA, BR	10
262961	INFOWEB SERVIÇOS E ENTRETENIMENTO LTDA - ME, BR	5	264070	FARIA & SCHIMITH LTDA - ME, BR	8
263859	PREFEITURA MUNICIPAL DE PARAUAPEBAS, BR	4	263085	VIA FIBRA NET TELECOM LTDA - ME, BR	7
52408	ITECH SOLUCIONES S.A, CR	4	21538	IGWAN-BL-AS - IGWAN.NET, BL	5
263580	EVEREST SOLUÇÕES EM TELECOMUNICAÇÕES LTDA, BR	4	52408	ITECH SOLUCIONES S.A, CR	5

Source: ‹https://bgpstream.com›

Table 9: LAC autonomous systems that caused the highest number of hijacks.

2017			2018		
ASN	Description	Hijacks	ASN	Description	Hijacks
263444	OPEN X TECNOLOGIA LTDA, BR	50	28140	MAXIWEB INTERNET PROVIDER, BR	21
27884	CABLECOLOR S.A., HN	25	267604	REACH TELECOM, BR	11
28229	HARDONLINE LTDA, BR	10	27884	CABLECOLOR S.A., HN	9
262725	RG SILVEIRA LTDA, BR	8	263459	INTERLINK COMUNICAÇÃO VIRTUAL LTDA ME, BR	7
264979	FRISIA COOPERATIVA AGROINDUSTRIAL, BR	6	262589	INTERNEXA BRASIL OPERADORA DE TELECOMUNICAÇÕES S.A, BR	6
			267286	DJG PROVEDOR E SERVICOS DE TELECOMUNICACOES, BR	6

Source: ‹https://bgpstream.com›

Table 10: Autonomous systems that were the most affected by hijacks.

2017			2018		
ASN	Description	Hijacks	ASN	Description	Hijacks
13489	EPM TELECOMUNICACIONES S.A. E.S.P., CO	233	14259	GTD INTERNET S.A., CL	79
61440	DIGITAL ENERGY TECHNOLOGIES CHILE SPA, CL	11	265791	COOPERATIVA ELÉCTRICA LIMITADA OBERÁ, AR	4
11993	BANCO DO BRASIL S.A., BR	5	266390	TAJO TECNOLOGIA LTDA, BR	4
52568	TOOLSNET TELECOMUNICACOES LTDA - ME, BR	4	61440	DIGITAL ENERGY TECHNOLOGIES CHILE SPA, CL	3
52850	M & M TELECOMUNICAÇÕES LTDA, BR	4	28646	CONFEDERAÇÃO INT. DAS COOP. LIGADAS AO SICREDI, BR	3
52768	ALSOL PROVEDOR DE INTERNET LTDA., BR	4			
262544	SULCOM INFORMÁTICA LTDA, BR	4			
27730	BBVA BANCO FRANCÉS SA, AR	4			

Source: ‹https://bgpstream.com›

Mitigation Strategies

While the BGP was designed without taking into consideration security aspects, not everything is nowadays up to the network operators' good will and trust. Over time, various strategies have been implemented to mitigate the effects of wrong routing announcements.

Firstly, constant monitoring is important. Operators cannot control what is being announced on the other side of the network nor check whether their prefixes are being correctly routed, but they can verify what is being announced through the BGP announcement collectors at different network points. This way, operators can take proactive action when they see some of their prefixes are being announced incorrectly at some point. For example, they can contact the provider causing the incident.

In addition, filtering announced prefixes is another key measure. Most networks only have to accept prefix announcements when it is necessary, and announce their prefixes to certain peers and not to the entire Internet. It is even possible to detect hijacks by monitoring, for example, changes in latency, network performance degradation or Internet traffic diversions.

To avoid relying just on the trust that the prefix announcements made by an autonomous system are legitimate, databases have been created, in which this information can be registered, delegating that trust to entities called Internet Routing Registries (IRRS). Thus, operators are able to register their ASNs and the prefixes they announce. This information can be accessed by other operators to filter BGP announcements and discard the ones that do not match the registered data. Nevertheless, security is not a guarantee with the IRRS: There is no unique registry, so not all the prefixes are registered in one single place. They may even contain mistakes, so some registries are better than others.[23]

[23] ‹https://blog.cloudflare.com/rpki/›

In an effort to trust the route announcements made by autonomous systems, encryption came into play and public key infrastructure standards were adopted. Successfully, trust issues were solved on other Internet layers, like TLS/SSL, which encrypts and authenticates HTTP sessions, for example.

Thus, the RPKI (Resource Public Key Infrastructure) system allows to couple an IP address range to an autonomous system number through cryptographic signatures. This infrastructure is made up of five Regional Internet Registries (RIRS): ARIN, RIPE NCC, APNIC, LACNIC and AFRINIC. Each one of these is a root certifying authority that issues the corresponding certificates when allocating resources.[24]

In short, each operator can create a Route Origination Authorization (ROA), which couples an ASN to the prefix it can announce, together with the possible maximum length of the prefix, in order to avoid hijacks caused by announcements that are more specific. These ROAS are digitally signed by the owner of that IP address space. This means that they can only be created with the approval of some RIR and, generally, they must be renewed every year.

Certificates and ROAS are published in a public repository, which can be accessed by different operators to get the validation they need to filter incorrect BGP announcements. These announcements are either originated by an incorrect ASN or they are more specific than is allowed, according to the policy established by the owner of each IP address block.

While this technology is available for all operators, it is not widespread yet. Nowadays, fewer than 20% of BGP announcements made across the network have their corresponding ROA to guarantee their authenticity.[25]

RPKI is an effective protection against attacks like autonomous system hijacks, which fraudulently announce prefixes they do not have. However, let us not forget that, with the BGP, both a false origin and a false route can be announced. A malicious network would still be able to fraudulently announce a route with a final destination to the ASN that is in fact coupled to the desired prefix through a ROA. With the RPKI this would not be detected, since it does not verify every link in the announced route, but only the final destination. As a response to this, the BGPSEC protocol was designed to ensure the route legitimacy of autonomous systems. This specification brings about important changes in the BGP, which require the update of hardware equipment. In turn, this will make its adoption slower.

---

[24] ‹https://www.noction.com/blog/rpki-overview›

[25] ‹https://observatory.manrs.org/›

Initiatives

SIDR (The Secure Inter-Domain Routing)

This initiative was introduced during the IETF 64 in 2005 and it was established as a working group in 2006. Its purpose is to reduce inter-domain routing system vulnerabilities. In particular, it seeks to ensure that autonomous systems only announce their authorized prefixes and to validate the generation of routes. This was the basis for the specification of AS route validation, which later became the BGPSEC.

SCION (Scalability, Control, and Isolation on Next-Generation Networks)[26]

As previously mentioned, the BGP was designed without taking into consideration security aspects. This led some research groups to search for completely disruptive solutions. SCION is an initiative originated at ETH Zurich, and it proposes a new Internet architecture, on the premise that solutions like the BGPSEC address the issue of route hijacking, but end up as solutions that lose scalability and create other issues, like a slower convergence. So, a clean-slate design is proposed to solve the fundamental problems.

SCION has already been implemented and it currently operates in some Swiss ISPs, although it seems highly unlikely for all operators to migrate to this architecture in the short- and medium-term.

MANRS (Mutually Agreed Norms for Routing Security)

MANRS is a global initiative launched by the Internet Society that provides fixes to reduce the most common routing threats. Its goal is to support two types of actors: network operators (ISPs) and Internet exchange points (IXPs). It promotes a series of actions that each of them must take in order to participate in the initiative. ISPs should deal with filtering, anti-spoofing, coordination and global validation. IXPs are encouraged to take these actions: prevent propagations, promote MANRS, protect the peering platform, enable the communication between ISPs and provide monitoring tools.[27]

---

[26] ‹https://www.scion-architecture.net/›

[27] ‹https://www.manrs.org/›

FORT Project

The FORT project[28] is a routing security initiative by LACNIC and NIC.MX for a free and open Internet. Its goal is to contribute to RPKI deployment to render routing systems more secure and resilient. The RPKI is a protocol that mitigates the vulnerabilities in these systems by facilitating a secure information exchange to prevent route hijacks. At the same time, FORT publishes data on routing incidents to show how routing system vulnerabilities affect Internet end users and their ability to enjoy a free and open Internet.

FORT offers three specific products:

- This report, which aims at assessing the number of routing incidents in the region and their impact on end users.
- The FORT Monitoring tool, which analyzes routing incidents in the region and reports intentional hijacks. This tool may be consulted by decision makers and operators in the region.
- The FORT Validator, a public key infrastructure validator for Internet number resources (RPKI). This is an open source validator. It was designed and developed to maximize the efficiency in the use of resources when being executed.

[28] ‹https://fortproject.net/›

Conclusion

In the next few years, over five billion people will be connected to the Internet. A great number of these new users lives in severely censored societies.[29] While this censorship can be conducted through different technical strategies and at different levels on Internet layers, there have been countless cases in which the attacks took place on the routing layer. This is possible by taking advantage of the vulnerabilities that the BGP did not foretell in its design, since it was developed for a network that was very different from today's, in which one could trust that all operators would act appropriately.

At present, with over 92,000 autonomous systems, it is necessary to adopt security measures, as a vulnerable routing infrastructure affects Internet freedom. This has been seen in incidents that have had serious repercussions, such as the 2008 Pakistani hijack or even in cases in the region, like the ones in Brazil in 2017.

Considering the number of incidents, there has been a downward trend since 2018. At the global level, incidents went from over 15,000 in 2017 to fewer than 13,000 last year. In our region, this decline is even steeper: from 5,000 to a little over 3,000. This may be attributed to the actions taken by organizations like NIC.BR, who have been working with network operators to take measures regarding route filtering and, thus, mitigate BGP incidents.

Over 70% of Latin American incidents take place in Brazil. It is the second country with the highest number of registered ASNs (the United States is in the first place), so a large portion of the statistics in the region rely on the behavior of its network operators. The situation is improving in this country, and most countries in Latin America and the Caribbean have improved compared to the previous two years.

Nonetheless, this reduction in the number of incidents in the region does not mean that we can be overconfident and assume that the issue has been solved. It is still necessary for every stakeholder to commit in order to achieve a secure and resilient network. Governments must provide a censor-free space and formulate policies for the deployment of technologies that help build a secure and reliable network, which is only possible if we have an active technical community that seeks to solve the vulnerabilities in current protocols, through standards like the BGPSEC and RPKI.

Additionally, it is essential for the civil society to continue monitoring and registering the connectivity abnormalities experienced by the different communities in order to report them when appropriate. All these efforts will be futile if the protagonists, i.e., the network operators in our region, do not do their jobs to strengthen the routing system. Today, they have the tools to do it: They can create their prefix ROAs obtained through the LACNIC portal, validate them using the FORT Validator, and monitor incidents using the FORT Monitoring tool.

[29] ‹https://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html›

Annexes

Number of Incidents by Month around the World

Date	Outages	Leaks	Hijacks
Jan 2017	620	111	139
Feb 2017	694	183	213
Mar 2017	722	136	301
Apr 2017	840	143	304
May 2017	907	189	170
Jun 2017	850	133	167
Jul 2017	1038	326	155
Aug 2017	993	811	193
Sep 2017	922	198	220
Oct 2017	1011	177	184
Nov 2017	812	225	199
Dec 2017	817	216	182
Jan 2018	718	210	181
Feb 2018	711	168	98
Mar 2018	804	218	0
Apr 2018	724	165	63
May 2018	668	213	230
Jun 2018	696	141	302
Jul 2018	627	149	407
Aug 2018	457	137	239
Sep 2018	524	155	236
Oct 2018	548	246	195
Nov 2018	647	392	249
Dec 2018	738	208	135
Jan 2019	782	270	143
Feb 2019	518	171	144
Mar 2019	604	247	133
Apr 2019	586	252	200

2017 Statistics

CC	Country	Outages	Leaks (culprit)	Leaks (victim)	Leaks (prop.)	Hijacks (culprit)	Hijacks (victim)	Active ASNs
AD	Andorra	3	0	0	0	0	0	1
AE	United Arab Emirates	18	0	1	5	2	5	57
AF	Afghanistan	16	0	6	0	4	6	41
AL	Albania	9	1	6	1	0	0	53
AM	Armenia	32	0	4	0	1	0	56
AO	Angola	12	5	3	0	4	1	38
AR	Argentina	271	0	11	0	35	18	598
AS	American Samoa	0	0	0	0	0	2	1
AT	Austria	4	84	6	12	6	13	469
AU	Australia	28	17	31	2	24	26	1372
AW	Aruba	0	3	0	0	0	0	1
AZ	Azerbaijan	75	0	1	1	1	1	43
BA	Bosnia and Herzegovina	12	3	2	0	0	3	31
BD	Bangladesh	110	78	114	10	17	23	438
BE	Belgium	6	1	2	9	4	6	202
BF	Burkina Faso	34	1	5	0	0	1	8
BG	Bulgaria	129	1	5	1	22	21	561
BH	Bahrain	0	0	0	0	0	1	17
BI	Burundi	0	0	0	0	0	2	9
BJ	Benin	12	0	1	0	3	4	11
BL	Saint Barthélemy	0	0	1	0	1	0	3
BM	Bermuda	0	0	1	0	0	1	15
BN	Brunei Darussalam	8	0	0	0	0	0	6
BO	Bolivia	81	0	3	0	3	2	25
BR	Brazil	2816	322	252	89	441	191	4914
BS	Bahamas	1	0	0	0	0	0	6
BT	Bhutan	1	0	1	0	0	0	6
BW	Botswana	19	0	1	0	1	2	17
BY	Belarus	41	0	2	0	7	0	92
BZ	Belize	1	0	0	0	2	2	10
CA	Canada	24	55	21	14	22	38	1159
CD	Democratic Republic of the Congo	0	3	9	0	4	6	16
CF	Central African Republic	7	0	9	0	0	0	2
CG	Congo	50	0	0	0	1	1	10
CH	Switzerland	9	16	10	6	7	16	593
CI	Côte d´Ivoire	7	10	2	0	3	0	12
CK	Cook Islands	56	0	1	0	0	0	1
CL	Chile	39	1	1	1	4	30	176
CM	Cameroon	28	0	3	0	1	3	14
CN	China	104	332	18	245	17	70	364
CO	Colombia	28	0	2	7	9	237	114
CR	Costa Rica	12	6	8	0	2	5	58
CV	Cape Verde	11	0	0	0	0	0	3
CW	Curaçao	0	0	0	0	0	2	16
CY	Cyprus	2	0	1	0	1	2	58

CZ	Czechia	4	3	8	5	8	9	482
DE	Germany	51	20	18	40	51	89	1637
DJ	Djibouti	16	0	0	0	0	0	2
DK	Denmark	0	0	0	0	3	5	264
DO	Dominican Republic	47	0	2	0	0	1	26
DZ	Algeria	51	0	1	0	1	0	9
EC	Ecuador	33	2	3	2	7	8	67
EE	Estonia	1	0	2	0	1	3	78
EG	Egypt	55	0	4	0	1	2	57
ER	Eritrea	1	0	1	0	0	0	1
ES	Spain	58	4	6	4	22	32	677
ET	Ethiopia	175	0	0	0	0	0	1
EU	European Union	0	7	0	44	1	1	31
FI	Finland	1	0	0	0	3	7	215
FJ	Fiji	12	0	2	0	2	0	7
FK	Falkland Islands	3	0	0	0	0	0	0
FR	France	28	65	11	90	19	52	978
GA	Gabon	22	3	13	0	0	0	11
GB	United Kingdom and Northern Ireland	43	70	35	65	87	109	1626
GE	Georgia	31	2	5	1	1	7	72
GF	French Guiana	7	0	0	0	1	0	4
GH	Ghana	18	28	14	10	9	1	48
GI	Gibraltar	0	0	1	0	0	0	8
GM	The Gambia	2	0	0	0	0	2	8
GP	Guadeloupe	0	0	1	0	0	1	2
GQ	Equatorial Guinea	3	0	1	0	0	0	6
GR	Greece	0	0	1	0	1	0	129
GT	Guatemala	2	0	2	0	4	9	33
GU	Guam	0	1	1	0	1	0	7
GY	Guyana	1	0	0	0	0	0	3
HK	Hong Kong	76	72	62	116	38	34	412
HN	Honduras	21	0	0	0	30	5	59
HR	Croatia	1	1	1	4	0	1	111
HT	Haiti	6	0	0	0	0	0	6
HU	Hungary	3	3	0	5	1	3	190
ID	Indonesia	307	26	71	5	44	20	895
IE	Ireland	2	0	1	0	2	10	154
IL	Israel	19	1	32	0	63	9	222
IM	Man Island	0	0	1	0	1	0	6
IN	India	403	90	201	66	104	85	1389
IO	British Indian Ocean Territory	22	0	0	0	0	0	1
IQ	Iraq	124	5	17	2	10	13	82
IR	Iran	605	5	64	5	84	62	430
IS	Iceland	0	0	2	0	1	0	58
IT	Italy	41	2	9	101	8	22	781
JM	Jamaica	1	0	0	0	5	0	8
JO	Jordan	4	1	0	0	3	1	31
JP	Japan	6	63	3	26	4	26	574
KE	Kenya	61	10	7	1	1	3	69
KG	Kyrgyzstan	28	1	1	1	0	0	27

KH	Cambodia	5	2	12	0	1	0	55
KI	Kiribati	38	0	0	0	0	0	2
KM	Comoros	5	0	0	0	0	0	2
KN	Saint Kitts and Nevis	0	0	0	0	1	0	1
KP	North Korea	10	0	0	0	1	0	1
KR	South Korea	79	0	31	1	27	19	692
KW	Kuwait	19	1	1	0	1	1	57
KY	Cayman Islands	0	0	0	0	0	2	9
KZ	Kazakhstan	22	16	12	12	9	12	91
LA	Lao People's Democratic Republic	0	0	13	0	0	0	14
LB	Lebanon	37	1	9	0	2	7	111
LK	Sri Lanka	3	4	6	0	1	1	13
LR	Liberia	1	0	0	0	0	0	8
LS	Lesotho	1	0	0	0	0	0	6
LT	Lithuania	1	0	1	0	4	11	112
LU	Luxembourg	3	0	0	0	2	1	71
LV	Latvia	3	3	1	0	2	10	217
LY	Libya	2	0	0	0	0	0	5
MA	Morocco	7	0	3	3	0	0	10
MD	Republic of Moldova	6	0	3	0	16	20	107
ME	Montenegro	1	0	0	0	0	1	13
MF	Saint Martin (French side)	0	0	1	0	3	0	3
MG	Madagascar	37	0	0	0	1	0	4
MH	Marshall Islands	4	0	0	0	0	0	1
MK	Former Yugoslav Republic of Macedonia	12	0	1	1	0	0	39
MM	Myanmar	4	70	88	4	1	1	36
MN	Mongolia	2	0	0	0	0	0	37
MO	Macao	0	0	6	0	0	0	6
MR	Mauritania	5	0	0	1	0	1	3
MT	Malta	5	0	0	0	0	1	27
MU	Mauritius	4	1	1	6	0	2	16
MV	Maldives	6	0	1	0	0	2	8
MW	Malawi	15	1	2	0	0	1	8
MX	Mexico	28	4	9	1	1	4	233
MY	Malaysia	2	18	17	0	12	8	161
MZ	Mozambique	63	0	2	0	0	2	20
NA	Namibia	2	1	1	1	0	0	8
NC	New Caledonia	2	0	2	0	0	0	8
NE	Niger	6	0	4	0	1	3	6
NF	Norfolk Island	2	0	0	0	0	0	1
NG	Nigeria	168	54	39	35	6	4	133
NI	Nicaragua	66	0	1	0	5	4	21
NL	The Netherlands	24	19	18	6	53	74	741
NO	Norway	4	2	1	16	4	14	261
NP	Nepal	14	6	6	0	3	0	56
NR	Nauru	1	0	0	0	0	0	2
NU	Niue	1	0	0	0	0	0	0
NZ	New Zealand	4	0	6	0	3	6	347
OM	Oman	9	0	2	0	0	0	10
PA	Panama	42	0	2	0	3	2	77

PE	Peru	84	0	0	0	2	4	28
PF	French Polynesia	8	0	0	0	0	0	3
PG	Papua New Guinea	101	5	5	0	0	0	11
PH	Philippines	12	40	83	9	18	4	246
PK	Pakistan	74	1	5	0	0	3	101
PL	Poland	20	6	12	1	18	34	1907
PR	Puerto Rico	32	5	4	0	5	0	48
PS	State of Palestine	44	0	13	0	3	4	39
PT	Portugal	2	0	2	3	6	1	75
PW	Palau	16	0	0	0	0	0	3
PY	Paraguay	65	0	1	0	1	0	38
QA	Qatar	0	0	0	1	0	0	9
RE	Réunion	1	0	0	0	0	0	3
RO	Romania	63	19	19	6	11	10	1049
RS	Serbia	22	7	7	2	0	5	148
RU	Russian Federation	450	190	129	152	222	92	4594
RW	Rwanda	2	1	4	0	0	0	12
SA	Saudi Arabia	83	13	6	2	4	7	116
SB	Solomon Islands	57	0	3	0	0	0	4
SC	Seychelles	19	0	2	0	0	0	12
SD	Sudan	15	0	0	0	0	0	6
SE	Sweden	11	3	7	253	14	16	528
SG	Singapore	22	102	12	102	30	28	251
SH	Saint Helena	5	0	0	0	0	0	0
SI	Slovenia	0	10	9	7	0	0	249
SK	Slovakia	1	1	1	1	0	0	139
SL	Sierra Leone	3	0	1	0	1	1	10
SO	Somalia	27	0	0	0	0	0	11
SR	Suriname	8	0	0	0	0	0	2
SS	South Sudan	0	0	1	0	0	0	6
SV	El Salvador	16	0	0	0	1	0	25
SX	Saint Martin (Dutch side)	1	0	0	0	0	0	3
SY	Arab Kingdom of Syria	27	0	0	0	0	1	2
SZ	Eswatini	5	0	0	0	0	0	7
TD	Chad	16	0	3	0	0	0	6
TG	Togo	19	0	0	0	0	0	3
TH	Thailand	37	14	53	8	11	17	336
TJ	Tajikistan	8	1	0	0	2	1	7
TL	Timor-Leste	27	0	2	0	0	0	5
TM	Turkmenistan	7	1	1	0	0	0	3
TN	Tunisia	60	0	0	0	0	0	12
TO	Tonga	0	0	0	0	0	2	3
TR	Turkey	91	7	12	2	10	19	408
TT	Trinidad and Tobago	14	0	1	0	2	1	13
TV	Tuvalu	1	0	0	0	0	0	1
TW	Taiwan	6	8	20	1	7	8	128
TZ	United Republic of Tanzania	37	0	0	0	10	4	57
UA	Ukraine	159	14	33	2	32	65	1628
UG	Uganda	55	0	0	0	0	3	27
UM	The United States Minor Outlying Islands	1	0	0	0	0	0	0

US	United States of America	776	744	835	1675	476	420	16380
UY	Uruguay	12	0	0	0	0	0	20
UZ	Uzbekistan	7	0	0	0	0	13	35
VE	Venezuela	5	6	12	0	1	1	52
VG	British Virgin Islands	0	0	0	0	1	0	4
VI	United States Virgin Islands	4	0	2	0	1	2	6
VN	Vietnam	27	19	36	7	8	8	224
VU	Vanuatu	4	0	0	0	0	0	8
WS	Samoa	7	0	1	0	0	0	4
YE	Yemen	3	0	1	0	0	0	2
ZA	South Africa	87	4	4	14	11	18	311
ZM	Zambia	2	0	0	0	6	2	15
ZW	Zimbabwe	23	0	4	0	0	0	16
ZZ	Non-registered	149	0	52	0	79	46	0

2018 Statistics

CC	Country	Outages	Leaks (culprit)	Leaks (victim)	Leaks (prop.)	Hijacks (culprit)	Hijacks (victim)	Active ASNs
AD	Andorra	0	0	0	0	2	0	1
AE	United Arab Emirates	9	0	0	0	2	3	59
AF	Afghanistan	24	0	8	0	3	7	44
AL	Albania	12	0	2	0	1	2	57
AM	Armenia	3	5	0	1	0	1	62
AO	Angola	14	6	0	0	131	0	43
AQ	Antarctica	1	0	0	0	0	0	0
AR	Argentina	267	1	8	1	21	18	716
AS	American Samoa	20	0	0	0	0	0	2
AT	Austria	3	7	9	9	7	12	491
AU	Australia	67	29	22	4	36	21	1437
AW	Aruba	1	0	0	0	0	0	1
AZ	Azerbaijan	26	0	6	2	0	0	44
BA	Bosnia and Herzegovina	2	0	4	0	0	0	33
BD	Bangladesh	83	263	309	106	16	35	582
BE	Belgium	7	0	8	5	10	10	212
BF	Burkina Faso	11	0	9	0	0	2	13
BG	Bulgaria	97	24	16	8	21	6	598
BH	Bahrain	0	3	2	0	0	1	18
BI	Burundi	0	0	0	0	0	2	9
BJ	Benin	12	7	0	0	0	0	12
BL	Saint Barthélemy	0	0	5	0	0	0	3
BM	Bermuda	0	0	0	0	0	2	14
BN	Brunei Darussalam	2	0	0	0	0	0	6
BO	Bolivia	38	0	0	0	1	0	30
BR	Brazil	1847	145	177	78	214	132	5941
BS	Bahamas	6	0	0	0	0	0	5
BW	Botswana	16	0	0	0	0	0	19
BY	Belarus	17	1	1	1	2	2	100
BZ	Belize	0	1	2	0	2	1	17
CA	Canada	25	13	11	12	42	35	1188
CD	Democratic Republic of the Congo	0	2	5	0	5	5	22
CF	Central African Republic	2	0	0	0	0	0	2
CG	Congo	16	0	0	0	1	3	9
CH	Switzerland	11	15	14	12	15	13	608
CI	Côte d´Ivoire	5	0	3	0	1	0	11
CK	Cook Islands	49	0	1	0	0	0	1
CL	Chile	22	0	2	0	10	91	220
CM	Cameroon	38	0	3	0	1	0	15
CN	China	36	33	35	85	36	125	395
CO	Colombia	25	17	3	0	15	8	127
CR	Costa Rica	3	6	7	0	3	3	67
CU	Cuba	1	0	0	0	0	0	3
CV	Cape Verde	1	0	0	0	0	0	3
CY	Cyprus	18	1	5	0	3	4	61

CZ	Czechia	6	6	12	2	4	8	505
DE	Germany	51	30	34	32	170	87	1746
DJ	Djibouti	6	6	0	0	20	0	2
DK	Denmark	4	0	1	0	1	3	272
DM	Dominica	0	0	2	0	0	0	2
DO	Dominican Republic	28	0	0	0	1	2	32
DZ	Algeria	14	0	1	0	0	1	9
EC	Ecuador	16	0	1	0	7	7	89
EE	Estonia	7	0	0	0	2	5	96
EG	Egypt	24	0	4	0	0	4	59
ER	Eritrea	2	0	0	0	0	0	1
ES	Spain	56	2	4	4	34	30	753
ET	Ethiopia	52	0	0	0	0	2	1
EU	European Union	0	5	0	38	0	3	38
FI	Finland	0	4	4	4	3	7	230
FJ	Fiji	20	0	2	0	0	0	10
FK	Falkland Islands	6	0	0	0	0	0	0
FM	Micronesia	0	0	0	0	0	1	4
FO	Faroe Islands	0	0	0	0	1	0	3
FR	France	23	20	10	145	15	36	1043
GA	Gabon	6	2	1	0	1	0	11
GB	United Kingdom and Northern Ireland	53	17	25	46	61	133	1683
GD	Grenada	2	0	0	0	0	2	4
GE	Georgia	15	8	3	0	0	6	82
GF	French Guiana	7	0	0	0	0	0	4
GH	Ghana	14	19	7	1	4	0	57
GL	Greenland	0	0	4	0	0	0	1
GM	The Gambia	1	0	0	0	0	0	8
GN	Guinea	0	0	1	0	0	0	8
GQ	Equatorial Guinea	2	0	0	0	0	0	6
GR	Greece	1	30	4	0	0	2	129
GS	South Georgia and the South Sandwich Islands	1	0	0	0	0	0	0
GT	Guatemala	2	0	0	1	0	8	36
GU	Guam	1	1	0	0	0	0	8
GW	Guinea-Bissau	1	0	0	0	0	0	2
GY	Guyana	2	0	0	0	0	0	4
HK	Hong Kong	51	58	52	93	55	65	448
HN	Honduras	4	0	0	0	9	8	62
HR	Croatia	1	135	2	1	0	0	113
HT	Haiti	10	0	0	0	0	0	8
HU	Hungary	3	0	0	0	0	4	195
ID	Indonesia	258	36	58	17	24	16	1024
IE	Ireland	5	0	2	0	5	8	159
IL	Israel	20	0	15	0	24	10	230
IN	India	371	236	47	57	78	119	1589
IO	British Indian Ocean Territory	6	0	0	0	0	0	1
IQ	Iraq	217	9	22	2	8	10	98
IR	Iran	414	3	23	3	61	59	429
IS	Iceland	0	0	1	0	0	1	62
IT	Italy	46	0	6	61	4	19	841

JE	Jersey	1	0	1	0	1	0	3
JM	Jamaica	0	0	0	0	2	1	8
JO	Jordan	7	22	2	0	0	0	34
JP	Japan	6	52	3	10	8	33	593
KE	Kenya	45	2	3	0	3	2	77
KG	Kyrgyzstan	23	0	1	1	4	3	27
KH	Cambodia	3	6	12	3	1	6	70
KI	Kiribati	48	0	0	0	0	0	2
KM	Comoros	21	0	0	0	0	0	2
KP	North Korea	2	0	0	0	0	0	1
KR	South Korea	38	3	10	3	17	39	700
KW	Kuwait	7	0	2	0	0	4	58
KY	Cayman Islands	0	0	0	0	0	2	9
KZ	Kazakhstan	24	3	8	3	1	4	96
LA	Lao People's Democratic Republic	0	2	2	0	0	0	16
LB	Lebanon	31	0	5	0	4	10	120
LC	Saint Lucia	3	0	0	0	0	0	2
LI	Liechtenstein	0	1	2	0	0	1	21
LK	Sri Lanka	14	3	3	0	0	1	14
LR	Liberia	9	0	0	0	2	1	9
LS	Lesotho	1	0	0	0	0	0	6
LT	Lithuania	5	1	4	1	3	6	123
LU	Luxembourg	0	0	0	0	2	4	73
LV	Latvia	13	1	0	0	3	6	217
LY	Libya	2	0	0	0	0	0	5
MA	Morocco	28	0	1	1	2	2	12
MD	Republic of Moldova	10	0	5	0	6	8	120
MF	Saint Martin (French side)	1	0	0	0	0	0	4
MG	Madagascar	45	0	0	0	0	1	4
MK	Former Yugoslav Republic of Macedonia	1	0	0	0	0	1	43
ML	Mali	0	0	0	0	3	0	6
MM	Myanmar	1	70	83	6	2	2	57
MN	Mongolia	12	0	0	0	0	0	37
MO	Macao	0	0	2	0	0	0	7
MR	Mauritania	3	0	0	0	0	0	3
MT	Malta	7	0	0	0	0	1	28
MU	Mauritius	4	0	0	5	3	2	17
MV	Maldives	21	0	0	0	0	0	10
MW	Malawi	9	0	2	0	0	0	11
MX	Mexico	31	3	3	2	4	4	250
MY	Malaysia	8	4	23	6	26	15	179
MZ	Mozambique	27	0	0	0	6	0	20
NA	Namibia	2	0	0	0	0	2	9
NE	Niger	22	0	2	0	0	1	6
NF	Norfolk Island	29	0	1	0	0	0	1
NG	Nigeria	138	13	9	0	3	3	139
NI	Nicaragua	36	0	0	0	6	0	21
NL	The Netherlands	24	7	12	19	85	84	807
NO	Norway	1	0	2	12	0	4	278
NP	Nepal	10	0	1	0	2	2	70

NR	Nauru	17	0	0	0	0	0	2
NU	Niue	1	0	0	0	0	0	0
NZ	New Zealand	9	1	11	0	4	8	370
OM	Oman	0	0	0	0	1	1	12
PA	Panama	25	2	3	14	8	3	76
PE	Peru	9	0	0	0	4	3	30
PF	French Polynesia	16	0	0	0	0	0	3
PG	Papua New Guinea	16	0	2	0	0	1	10
PH	Philippines	9	37	51	2	31	9	250
PK	Pakistan	41	0	4	0	1	8	119
PL	Poland	41	9	12	5	171	32	1974
PM	Saint Pierre and Miquelon	2	0	0	0	0	0	1
PR	Puerto Rico	11	0	1	0	4	3	49
PS	State of Palestine	28	0	4	0	1	2	40
PT	Portugal	0	0	0	8	22	8	84
PY	Paraguay	112	0	0	0	1	0	50
QA	Qatar	0	0	0	0	0	1	10
RO	Romania	69	10	24	6	15	16	1037
RS	Serbia	34	0	2	0	4	1	151
RU	Russian Federation	274	120	160	112	63	62	4699
RW	Rwanda	0	0	1	0	0	0	12
SA	Saudi Arabia	10	52	9	3	1	4	123
SB	Solomon Islands	139	0	1	0	0	0	3
SC	Seychelles	12	0	1	0	0	0	11
SD	Sudan	36	0	2	0	0	0	6
SE	Sweden	18	7	4	38	7	6	539
SG	Singapore	33	12	9	192	9	24	269
SH	Saint Helena	18	0	0	0	0	0	0
SI	Slovenia	0	4	4	2	1	0	251
SK	Slovakia	1	0	0	0	0	0	147
SL	Sierra Leone	2	0	0	0	0	0	13
SM	San Marino	3	0	0	0	0	0	6
SN	Senegal	0	0	0	0	0	1	6
SO	Somalia	1	0	0	0	0	0	12
SR	Suriname	14	0	0	0	0	0	3
SS	South Sudan	0	0	2	0	0	1	6
ST	Saint Thomas and Prince	1	0	0	0	0	0	2
SV	El Salvador	7	0	1	0	1	2	27
SY	Arab Kingdom of Syria	26	0	0	0	0	0	2
SZ	Eswatini	4	0	0	0	2	0	7
TD	Chad	6	0	0	0	0	0	8
TG	Togo	0	0	5	0	0	0	4
TH	Thailand	25	14	10	4	5	10	351
TJ	Tajikistan	17	1	0	0	0	1	7
TL	Timor-Leste	9	0	3	0	0	0	6
TM	Turkmenistan	20	0	0	0	0	0	4
TN	Tunisia	53	0	1	0	0	1	15
TR	Turkey	82	5	6	4	18	14	425
TT	Trinidad and Tobago	13	0	2	0	2	1	14
TW	Taiwan	9	3	8	3	6	14	141

TZ	United Republic of Tanzania	19	1	4	0	4	5	60
UA	Ukraine	134	11	21	1	33	35	1578
UG	Uganda	6	0	1	0	0	4	28
UM	The United States Minor Outlying Islands	1	0	0	0	0	0	0
US	United States of America	685	681	772	1526	408	522	16688
UY	Uruguay	4	0	0	0	2	0	19
UZ	Uzbekistan	11	0	0	0	0	1	36
VE	Venezuela	8	0	1	0	2	1	54
VG	British Virgin Islands	0	0	0	0	1	0	6
VI	United States Virgin Islands	11	0	0	0	0	1	6
VN	Vietnam	11	26	12	3	10	10	242
VU	Vanuatu	30	0	0	0	0	0	9
WF	Wallis and Futuna Islands	6	0	0	0	0	0	1
WS	Samoa	18	0	1	0	0	0	4
YE	Yemen	4	0	0	0	0	0	3
ZA	South Africa	121	7	2	5	21	19	368
ZM	Zambia	2	0	1	0	2	1	14
ZW	Zimbabwe	19	0	0	0	0	0	18
ZZ	Non-registered	60	0	15	0	77	33	0